CCDCOE

NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Pascal Brangetto, Emin Çalişkan, Henry Rõigas

Cyber Red Teaming

Organisational, technical and legal implications in a military context

Tallinn 2015

www.ccdcoe.org
publications@ccdcoe.org

Table of Contents

Executive summary **4**

Introduction **6**

1. Aim, scope, definitions and methodology **10**

Aim of the study **10**

Scope and definitions **10**

Methodology & caveats **15**

2. Organisational and policy considerations of cyber red teaming activities **16**

Frameworks for cyber red teaming **16**

Assembling the cyber red team **18**

Skill requirements for cyber red teams **21**

Making cyber red teaming valuable & mitigating the risks **23**

3. Technical considerations for cyber red teaming activities **27**

Infrastructure Design and Operational Environment **27**

a. ‘Operational Environment’ 27

b. Cyber Ranges 29

Execution: putting the cyber red team into play **32**

a. Defence in Depth 33

a. Attack Flow 33

b. Tools 35

4. The legal implications of cyber red teaming activities **37**

Legal framework for the use of cyber red teams **37**

Legal risks of cyber red teaming activities **43**

a. Data protection, illegal interception and possible infringements of privacy laws 43

b. Liability issues – reparations 46

c. The case of reverse engineering. 48

Conclusion **49**

Executive summary

Cybersecurity is about managing risks and to ascertain that, to a certain extent, proper procedures and adequate security measures are being taken. Exposed to constant cyber threats, military organisations rely on a vast number of communication and information systems. They require the capacity to assess, on a regular basis, the successful deployment of these security measures.

Cyber red teams (CRT) – commonly performing penetration testing – focus on threats from adversaries in the cyber world. They mimic the mind-set and actions of the attacker in order to improve the security of one's own organisation. As a standing capability in a military environment, these tools can be used in order to enhance preparedness and improve training capacities.

Building on different doctrinal documents and best practices observed in the private sector, this study reviews the requirement and the possible barriers for military units to perform cyber red teaming. After clarifying the definition issues surrounding the notion of CRT, the study addresses and discusses the main policy, organisational, technical, and legal considerations regarding the implementation of military CRT. This study takes a broad approach as these implications are dependent on country-specific factors such as available resources and level of ambition for developing a cyber red teaming capability.

In considering cyber red teaming, a basic first step is to develop a clear procedural framework or a doctrine that will outline the need for a CRT within a military organisation. One of the main traits identified is that cyber red teaming is a technical endeavour and will mostly rely on high-level specialists with a wide range of skill-sets, involving therefore experts from the private sector. The issue of the recruitment is a salient one, because it does not only matter to the building-up of a CRT. The main observation is that a civil-military cooperation is inevitable to render a CRT effort worthwhile. Furthermore, there is also a need for a nation to reach a maturity level in the implementation of a cyber security strategy in order to consider these paths to explore.

From the technical standpoint, both operational and simulated (cyber ranges) environments for cyber red teaming are examined in the study. Choosing between the two options depends on the expected outcomes of a CRT assignment (e.g., cyber ranges will allow an organisation to evaluate and test certain offensive solutions in a harmless environment). While addressing the exploitation and the execution phase of the cyber red teaming process, this study provides for a list of common known tools used by a CRT. These tools can be either licensed or developed in-house. One of the main limitations is the fact that ready-to-use solutions might have unforeseeable consequences that can cause damage and harm, especially when tested on a "live" environment.

The section focusing on the legal implications first defines the provisions that are necessary to facilitate the implementation of a CRT capability. As such, as it is an

activity conducted “with authorisation” and pursuing a legitimate goal, it is deemed lawful when analysing the legal provisions of several NATO nations. In addition, they can provide regulatory provisions that protect the members of a CRT without criminalising their activities especially in regard with reverse engineering or malware design issues. Nevertheless, the study identified three main potential legal risks pertaining to CRT activities: infringements of privacy and intellectual property laws, and the liability issue in case of unforeseen consequences occurring following these activities. For the latter case, it is possible to exculpate the operators of a CRT while engaging the state responsibility without fault as certain CRT activities can be deemed dangerous by nature.

'If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle.'

Sun Tzu, The Art of War

Introduction

Alternative ways of thinking are of major importance among military organisations, as mind sets should be challenged on a daily basis in order to enhance the level of preparedness and, more importantly, to avoid complacency.[1] It is of paramount importance to tackle this difficult task; in fact, the pace of technical progress urges the military to always be, if not anticipating, then at least up to date in a significantly competitive environment. The cyber realm is one of those dimensions, and one in which military organisations are constantly confronted with new challenges.

Deriving from the Cold War, the expression 'red team' among the military is often used to describe a way to think outside the box and to be able to anticipate and model adversarial behaviour. Often, red teaming techniques were implemented in order to assess the vulnerabilities of certain military capabilities in a broader context.[2] The following definition, provided by the UK Ministry of Defence in 2013, can be useful in explaining the broader concept of red teaming. As shown here, this concept is used to provide a better insight with regard to the decision-making processes:

> *'A red team is a team that is formed with the objective of subjecting an organisation's plans, programmes, ideas and assumptions to rigorous analysis and challenge. Red teaming is the work performed by the red team in identifying and assessing, inter alia, assumptions, alternative options, vulnerabilities, limitations and risks for that organisation. Red teaming is a tool set. Using it will provide the end user (commander, leader, or manager) with a more robust baseline for decision making'.*[3]

Knowing the techniques, tactics and procedures of your adversaries in cyberspace can be a key to success, as it is often deemed that 'the offense has the upper hand'.[4]

---

[1] There are a number of examples of complacency in military history. For instance, due to a lack of imagination, the French command had not foreseen the fast paced evolution of military affairs before the Second World War. Complacency is generally considered to be one of the key explanations for the French defeat in 1940. See Marc Bloch, *The strange defeat-L'étrange défaite*, *témoignage écrit en 1940*, Éditions Gallimard, 1990.

[2] One of the major red team initiatives taken by the US Department of Defense was the implementation of a Navy red team, the US Navy's 'Red Cell' in charge of uncovering weaknesses in the security of the installations of the ballistic missile nuclear submarines (SSBN), see the Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities, September 2003, p. 4. https://www.fas.org/irp/agency/dod/dsb/redteam.pdf (all the links were last accessed January 14th 2015).

[3] *Red Teaming Guide*, UK Ministry of Defence, January 2013, p.9.

[4] William Lynn, 'Defending a new domain', *Foreign Affairs*, September – October 2010, Volume 89, p.99.

Red teaming in cyberspace is not a new phenomenon. Exercise Eligible Receiver[5], conducted in 1997, was a prominent example of a high-scale exercise led by an NSA red team that consisted of attacks on critical infrastructure networks, particularly energy providers and Command and Control capabilities. Eligible Receiver was a classified and non-notified exercise sponsored by the United States Department of Defense (US DoD) which included a large number of federal agencies including the Federal Bureau of Investigation. The impact of the exercise was significant as it served as a wake-up call among senior officials to improve cyber defence in the United States.

Today cyber red teams are often to be found in exercises and training sessions, as outlined by the US DoD.[6] The main purpose is to test the blue teams that are supposed to defend the networks rather than to focus on vulnerability assessments. There are numerous examples of such exercises, such as the Locked Shields exercise[7] hosted by the NATO Cooperative Cyber Defence Centre of Excellence in Estonia.

The protection of information systems is of deep concern as they are deemed vulnerable by nature. Cyberattacks are being conducted daily on any type of target, and any notion that a state of full cyber security can be reached is a mere illusion. To improve the level of security, an arsenal of solutions has been created and this includes vulnerability assessments.[8] Vulnerability assessments are an integral part of cybersecurity and can take a number of forms that range from security audits to penetration testing. Very similar in their approach, these tools are now part of any cyber security policy, whether applied in the private or the public sector. In the context of cyber security, the practice better known as penetration testing ('pentesting') or ethical hacking is part of the range of vulnerability assessment methods regarding information systems. In a sense, '[t]esting your own defenses has become a way of life'.[9] This is particularly true for cybersecurity as it provides

---

[5] Bill Gertz, *The Washington Times*, 16 April 1998. As Pentagon spokesman Ken Bacon said at the time, 'Eligible Receiver was an important and revealing exercise that taught us that we must be better organised to deal with potential attacks against our computer systems and information infrastructure.'

[6] 'Because degraded cyberspace operations for extended periods may be a reality and disruption may occur in the midst of a mission, DoD will fully integrate a complete spectrum of cyberspace scenarios into exercises and training to prepare U.S. Armed Forces for a wide variety of contingencies. A cornerstone of this activity will be the inclusion of cyber red teams throughout war games and exercises. Operating with a presumption of breach will require DoD to be agile and resilient, focusing its efforts on mission assurance and the preservation of critical operating capability.' Department of Defense Strategy for operating in cyberspace, July 2011 p.6, http://www.defense.gov/news/d20110714cyber.pdf.

[7] Kim Zetter and Pete Brook, 'Hackers Gather for Cyberwar in an Intense 48-Hour Sim', *Wired magazine*, October 10 2014, http://www.wired.com/2014/10/luca-locatelli-locked-shields/.

[8] 'White hats to the rescue', *The Economist*, 22nd February 2014, http://www.economist.com/news/business/21596984-law-abiding-hackers-are-helping-businesses-fight-bad-guys-white-hats-rescue.

[9] Zachary Fryer-Biggs, 'Building better cyber red teams', June 14 2012, http://www.defensenews.com/article/20120614/TSJ01/306140003/Building-Better-Cyber-Red-Teams.

relevant testing for personnel or procedures and allows the identification of the weakest points and thus the appropriate corrective measures.[10] Pentesting is a valuable addition to the arsenal of security solutions as it also generates awareness.

According to the United States National Institute of Standards and Technology, pentesting

> *'…is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network. It often involves launching real attacks on real systems and data that use tools and techniques commonly used by attackers. Most penetration tests involve looking for combinations of vulnerabilities on one or more systems that can be used to gain more access than could be achieved through a single vulnerability.'*[11]

The aims of pentesting and red teaming in general can be viewed as the same, as they are both focused on uncovering the vulnerabilities of an organisation. The authors of this study consider that *cyber* red teaming activities conducted in military organisations should be more focused on vulnerability assessments. This view is also expressed by Maj. Gen. Suzanne M. Vautrinot, who explained the cyber red team concept in the context of the US: '[it] focuses on vulnerability assessments and intrusion missions of DoD networks'.[12] The authors of this study also see the concept as being more applied on the technical rather than on the decision-making level, and it is important that the activity of cyber red teaming covers the simulation of a threat environment in order to make it as realistic as possible.

Military organisations are large and are dependent on a significant number of information systems. In fact, dependence on computer systems is so high that the loss of control of this infrastructure might lead to the inability to manoeuver and impair operational capabilities.[13] As General Keith B. Alexander put it, given the number of networks, it is practically impossible to be able to defend them all.[14] Thus, identifying the weakest points can enable to a better cybersecurity posture to be built. Military networks can also be deployed abroad during the conduct of operations,

---

[10] The case of Facebook is a good example of a well-implemented cyber security policy. See Dennis Fisher, 'How Facebook prepared to be hacked', *Threatpost*, 8 March 2013, http://threatpost.com/how-facebook-prepared-be-hacked-030813/77602.

[11] *Technical Guide to Information Security Testing and Assessment, Recommendations of the National Institute of Standards and Technology*, September 2008, p. 36, http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf.

[12] 'Digital warriors: improving military capabilities for cyber operation', Hearing before the subcommittee on emerging threats and capabilities of the committee on armed services, House of Representatives 112th Congress Session, hearing held on 25 July 2012, p 103.

[13] As an example, the US Army operates more than 400 network connections, 700 circuits, over 800,000, workstations, over 35,000 servers and over 90,000 mobile devices.

[14] Noah Schactmann, Military Networks 'Not Defensible,' Says General Who Defends Them, *Wired*, 1 December 2012, http://www.wired.com/2012/01/nsa-cant-defend/.

national or multinational. The global footprint of information systems urges policy makers to make sure that their networks are safe. In addition, the militarisation of cyberspace – a phenomenon that has been observed for the last ten years[15] – and the global role of military infrastructures in the governance of cyber security on the national level[16] shed new light on the role of military organisations in the endeavour to secure cyberspace.

This study intends to explore the organisational, technical, policy and legal aspects of the deployment of cyber red teaming capabilities in the military realm, analysing their possible drawbacks, shortcomings and risks. After defining the scope and definitions of cyber red teaming (Chapter 1), this study will address the organisational and policy issues (Chapter 2), and then analyse the technical (Chapter 3) and legal (Chapter 4) considerations related to the use of cyber red teams.

[15] Jeason Healey (Ed.), *A fierce domain: Conflict in cyberspace* 1986-2012,
[16] Ian Wallace, *The Military Role in National Cybersecurity Governance*, Brookings, 16 December 2013.

1. Aim, scope, definitions and methodology

This study is based on a Request for Support made to the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) initiated by the German Armed Forces.[17] This request was submitted to the NATO CCD COE steering committee and approved for implementation.

Aim of the study

The project description made the observation that red teaming and penetration testing are widely requested and offered services, especially in the private sector. As some states are considering developing similar assets in an effort to test their own or, on request, someone else's, level of security, the implementation of such a policy is frequently accompanied by questions regarding the legality of such actions and the technical and organisational requirements that need to be considered. This study is expected to help develop a wider understanding about whether or not barriers for military units to offer this service are in place, and what are the possible pitfalls or necessary requirements which must be taken into account.

Scope and definitions

In the lexicology of cyber security, there is a lack of clarity of the terms ‘cyber red teaming’, ‘penetration testing’ and even ‘vulnerability assessments’. Like many concepts and methods, common and operational definitions are difficult to come by as their dimension in the information security literature can be unclear. Depending on the authors, these concepts either overlap or are used interchangeably. In order to bring some clarity to the topic, the authors of this study have approached cyber red teaming through a number of doctrinal documents and official definitions so that common traits can be identified.[18]

---

[17] Federal Office of Bundeswehr Equipment, Information Technology and In-Service Support (Das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr BAINBw).

[18] ‘A DoD Cyber Red Team is a group of DoD personnel (military, civilian, contractor) authorised and organised to emulate a potential adversary’s exploitation or attack capabilities against a targeted mission or capability. DoD Cyber Red Teams operate to identify exposed information and vulnerabilities of the target’s security posture; support information assurance readiness; create a degraded, disrupted, or denied cyber environment; develop the skills and exercise capabilities of cyber forces; participate in evaluation of Computer Network Defense Service Providers (CNDSPs) and its subscribers; and provide Protect Services for CNDSPs or support OPSEC surveys. A DoD Cyber Red Team achieves its purpose by conducting cyberspace operations and limited supporting operations in the physical domains.’ Memorandum CJCSM 6510.03 28 February 2013 issued by the Chairman of the Joint Chiefs of Staff on the Department of Defense Cyber red Team Certification and Accreditation http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651003.pdf.
‘An organizational element comprised of trained and educated members that provide an independent capability to fully explore alternatives in plans and operations in the context of the operational environment and from the

The idea behind cyber red teaming is its scalability and its capacity to encompass and integrate the wide array of vulnerability assessments techniques. Based on the identified commonalities, a cyber red team is defined in this study as:

> **an element that conducts vulnerability assessments in a realistic threat environment and with an adversarial point of view, on specified information systems, in order to enhance an organisation's level of security.**

As the definition indicates, a cyber red team can be defined according to the following constitutive features:

- an element:

The authors see that cyber red teaming can be conducted either from an internal dedicated organised element, or outsourced to specialised contractors. The cyber red team can be a standing capacity or a more flexible and adaptable part of the organisation as determined by the set needs and priorities. This element could deploy a full spectrum of cyber techniques, whether immediately available or tailor-made, with regard to the target information system.

- that conducts vulnerability assessments:

In the view of the authors, vulnerability assessments encompass activities ranging from information security audits[19] to pentesting or ethical hacking.[20] The activity of cyber red teaming is viewed as mostly consisting of pentesting techniques (especially black-box pentesting[21]) but it might also include intrusion testing on physical facilities and real-life cyberattacks. Real-life cyberattacks are non-notified activities against an information system, such as situations when a cyber red team uses a series of techniques against a military Communication and Information Systems (CIS) in order to create an effect such as the theft of data. For the purposes of this study, and in accordance with NATO documents, a 'cyberattack' is understood to be '[a]n act or action initiated in cyberspace to cause harm by compromising communication,

---

perspective of adversaries and others.' *US Army Field Manual 3-38, Cyber-Electronic Activities*, February 2014, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf.

[19] '[T]he IS audit [German: IS-Revision] focuses on information security in the organisation. The goal of an IS audit is to have an independent party determine the current level of security throughout the organisation and point out any existing security gaps and deficiencies. The IS audit is a special type of the (general) audit. The result is an IS audit report with recommendations for improving the level of information security.' See the Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz, issued in 2008 by the German Federal Office for Information Security, p. 7.

[20] Penetration testing can also cover a wide set of activities such as social engineering, password cracking, using rootkits.

[21] In penetration testing, black-box testing refers to a methodology where an ethical hacker has no knowledge of the system being attacked. The goal of a black-box penetration test is to simulate an external cyberattack.

information or other electronic systems, or the information that is stored, processed or transmitted in these systems.'[22]

- in a realistic threat environment and with an adversarial point of view:

A cyber red team's work requires thorough intelligence work that gives knowledge of the adversary's techniques, mind-sets and goals in order to apply realistic attacks. In addition, by creating a degraded environment by, for example, denying access to certain services, cyber red teams enable operators to test their procedures when defending a network against cyberattacks.

- on specified information systems:[23]

Cyber red teams can be deployed on specified information systems. These information systems comprise tiers that may be military networks, government networks or critical infrastructure networks. In addition, the cyber red team activities are to be conducted 'with right', i.e. with authorisation.

[22] NATO 'Report on Cyber Defence Taxonomy and Definitions,' Enclosure 1 to 6200/TSC FCX 0010/TT-10589/Ser: NU 0289.

[23] An information system is a combination of hardware, software, infrastructure and trained personnel organised to facilitate planning, control, coordination, and decision-making in an organisation. It includes technologies, organisational requirements, procedures, personnel, physical security, information security, and – where applicable – electro-magnetic security.

Purpose	Functions	Examples
Understand	Help the organisation better understand the adversarial behaviour.	Intelligence gathering activities.
	Clarify the organisation's assumptions and expose its biases.	
Anticipate	Anticipate possible courses of action of the adversary.	Threat, risk and vulnerability assessments (implicit).
	Avoid surprise.	Military decision-making process revision.
	Better shape the organisation's courses of action.	
Test	Probe or penetrate the organisation's systems or security	Penetration testing (physical and IT).
	Identify and explore vulnerabilities	Exercises, experiments.
	Explore and test the organisation courses of action and countermeasures when confronted to a cyber red team activity.	
Train	Teaching and training.	Creation of a training centre. Dedicated infrastructures (cyber lab).
Report – Action on results	Inform the organisation	Document cyber red teaming activities.
	Recommendations	Applying software updates. Implement account and process auditing software. Create and promote information security awareness within the organisation.

Table 1- Red teaming purposes[24]

- <u>in order to enhance an organisation's level of security</u>:

The main goal of a cyber red team is to uncover vulnerabilities: this will enhance the level of security of an organisation by testing the structures, procedures and personnel of the organisation. The assessments that are conducted should therefore provide recommendations, follow-up actions and, when possible, corrective measures. Table 1 provides a brief overview of what could be achieved through cyber red teaming.

[24] This table is inspired by Mark Mateski, 'Toward a Red teaming Taxonomy 2.0', Red teaming journal, September 2004, http://redteamjournal.com/2008/09/toward-a-red-teaming-taxonomy-20/.

The main idea driving cyber red teaming is to be able to avoid relying on ready-made solutions and rigid and stagnant mind sets but rather to provide relevant methods in order to avoid complacency. It must be seen as a comprehensive process.

Diagram 1 below provides a presentation of the four main phases of the cyber red team cycle.

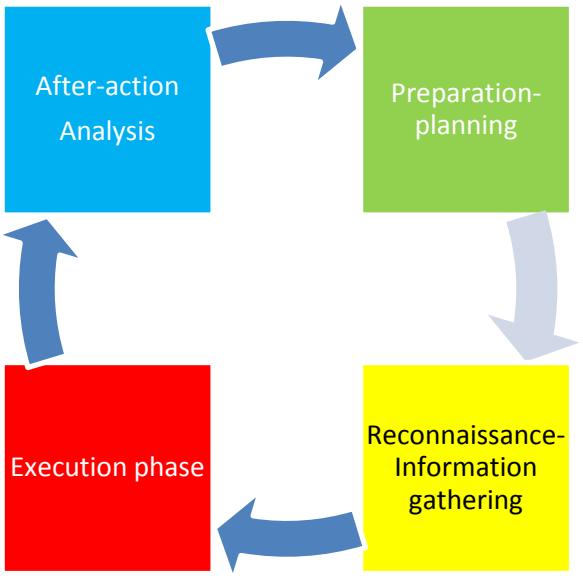

Figure 1 – Cyber Red team cycle[25]

- Planning and preparation: The rationale for cyber red teaming is to be defined during this phase. There is a need before engaging in any activity to assess the current needs of a specific organisation and the scope of the actions that will be undertaken. This is the phase during which limitations such as the duration, the legal boundaries and prohibited actions have to be determined. This can be compiled under the form of rules of conduct.
- Information gathering – Reconnaissance: This phase includes preliminary surveying or research of the targeted information system that can range from web research, social engineering and common techniques to more complex operations such as specific intelligence reports. This phase can also be used to gather and develop the tools required to access the targeted systems.
- Execution phase: This is the active part of the cyber red teaming process, when tools and know-how are deployed in order to uncover the vulnerabilities. These actions may range from port scanning, gaining access to escalation of privileges, and clearing tracks.

[25] Advanced Security Essentials, Attack process, p. 15, taken from the Security 501.3 booklet regarding Pentest.

- After-action analysis: During this phase, all the actions taken are documented, the results listed, and recommendations and proposals given. Follow-up actions can also be envisaged in which cyber red teams can be involved.

Methodology & caveats

The main difficulty of this study resided in the access to information regarding the practices of different states, especially in the military realm. Given the general sensitivity of the information involved, the unclassified information available on the subject of cyber red teaming or penetration testing in the military is limited. Therefore, it is important to highlight that the authors of this study relied on publicly available open source information. For this reason, the study is also heavily influenced by the information that the US has, to a certain extent, disclosed on the topic. Cyber defence practices in the US could be seen as a worthy example since the country is regarded as the first military power and one of the most advanced actors in cyber security, and concepts of cyber red teaming are a part of US cyber defence policy.

Despite its main focus being at the technical level, this study will also address general concerns pertaining to cyber security when dealing with governance issues. It aims to give a general overview and does not present an all-encompassing list of possible issues involved with military cyber red teaming. Neither does it go into detail in describing particular aspects as they are highly dependent on nation-specific requirements. This factor also applies to the definition of a cyber red team provided above: the use or development of cyber red teams depends on the nation's level of resources and ambition which can be, in turn, influenced by the will to take risks with regard to the possible negative effects of the activity.

2. Organisational and policy considerations of cyber red teaming activities

Chapter 2 will present commonly identified organisational and policy requirements and barriers related to the development or use of military cyber red teaming. It is divided into four sections: (1) policy and doctrinal frameworks; (2) the assembly of a cyber red team; (3) necessary skillsets; and (4) the value of cyber red teaming.

Frameworks for cyber red teaming

The concept of red teaming is subject to many interpretations and may encompass a wide set of activities depending on different contextual settings. Therefore, as a first step to achieve a military *cyber* red teaming capability, the notion has to be elaborated on and explained within the organisation. The purpose, scope, methodologies and processes of the cyber red teaming activities have to be clear so as to legitimise red teaming activities. This is especially important if one takes into account the possible perceptions that are associated with the use of red teams. For example, the conduct of military red teaming operations are seen as being hindered by a 'cultural resistance' within the organisation; that is a resistance from the targeted organisation to the prospect of an outside actor discovering and reporting failures in security.[26] With matters of cyber red teaming, the 'resistance' and the confusion might be even higher due to the general tendency to have limited knowledge of cyber threats.

The concept of red teaming could be elaborated through instruments such as policy and strategy documents, military doctrines, and explanatory reports.[27] As red teaming is a broader concept applied in the military, a cyber red teaming competence could be just a part of a wider set of red teaming capabilities. In the context of broader military red teaming activities, it is a general observation that there is little information on the topic in formal military doctrine and publications.[28] Nevertheless, some official publications can be highlighted. The 'Red Teaming Guide' (2013) by the UK Ministry of Defence describes the concept: the guide links red teaming mainly with an alternative and critical analysis of an organisation's or a commander's assumptions. A similar approach with an emphasis on decision-making and intellectual analysis is presented in several US doctrines and reports that mention red

[26] Scott Applegate, 'Full Spectrum Red Teaming in the Military Environment,' Student Paper Submitted for Cyber Security for Information Leaders (SEC 11-01), National Defense University, Information Resources Management College (iCollege), United States Army, November 26, 2010, p 11. https://www.academia.edu/1166995/Full_Spectrum_Red_Teaming_in_the_Military_Environment

[27] Examples provided in this section are based only on public unclassified documents available in English.

[28] Brendan Mulvaney, 'Red Teams. Strengthening through challenge,' *Marine Corps Gazette*, July 2012, http://www.hqmc.marines.mil/Portals/138/Docs/PL/PLU/Mulvaney.pdf.

teaming as part of military operations and planning.[29] Although these concepts can be linked with the basic purpose of *cyber* red teaming, they are mainly focusing on challenging norms by providing alternative analysis or an adversarial view to certain aspects of planning, and do not specifically cover activities related to *cyber* red teaming which mostly encompasses penetration testing of specified information systems.

Since cyber red team operations have a different, more technical nature in comparison to 'classical' or broader concepts of red teaming, it is fair to assume that an organisation has to develop a cyber-specific framework to achieve a military cyber red teaming capability. As there are only a limited number of official publications by the military on the topic of red teaming, there are even fewer doctrinal documents available on military *cyber* red teaming.[30] Some findings can still be highlighted.[31] The 'Department of Defense Strategy for Operating in Cyberspace' (2011) indicates the relevance of using red teams in exercises and training. In addition, although not presenting the official position of the U.S. Department of Defence (DoD), the 2013 report 'Resilient Military Systems and the Advanced Cyber Threat' by the Defence Science Board highlights the success rate of red teams in exercises and tests against DoD networks. The term 'red team' is also mentioned in the context of cyber security by officials in US Congress hearings.[32] In one of these hearings, the former NSA Director General Keith B. Alexander briefly mentions that red teaming provides an effective assessment of systems and gives an opportunity to use offensive capabilities for defence purposes.[33] This leads to the observation that a link with cyber red teaming can also be identified in the context of broader cyber defence strategies: for example, the prospect of using offensive capabilities for testing is

---

[29] Field Manual No. 5-0, The Operations Process, Headquarters, Department of the Army Washington, DC, 26 March 2010, http://fas.org/irp/doddir/army/fm5-0.pdf ;
Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics Washington, D.C., Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities, September 2003, http://fas.org/irp/agency/dod/dsb/redteam.pdf : University of Foreign Military and Cultural Studies, Red Team Handbook, 15 April 2011, http://www.au.af.mil/au/awc/awcgate/army/ufmcs_red_team_handbook_apr2011.pdf.

[30] For example, see Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune, Alain Esterle, Pablo Rodriguez, 'Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP). Unclassified Summary,' RAND Corporation, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR286/RAND_RR286.pdf.

[31] *Field Manual No. 3-38, Cyber Electromagnetic Activities*, Headquarters Department of the Army, Washington, DC, 12 February 2014, http://armypubs.army.mil/doctrine/DR_pubs/dr_a/pdf/fm3_38.pdf; *Department of Defense Cyber Red Team Certification and Accreditation*, Chairman of the Joint Chiefs of Staff Manual, 6510.03, 28 February 2013, http://www.dtic.mil/cjcs_directives/cdata/unlimit/m651003.pdf; *Department of Defence Strategy for Operating in Cyberspace*, Department of Defence, United States of America, July 2011, p.6, http://www.defense.gov/news/d20110714cyber.pdf.

[32] 'U.S. Cyber Command: Organizing for Cyberspace Operations," House hearing before the committe on Armed Services, 111 Congress, held 23 September 2010, http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62397/html/CHRG-111hhrg62397.htm.

[33] *Ibid.*

briefly mentioned in 'The Defence Cyber Strategy' published in 2012 by the Ministry of Defence of the Netherlands.[34]

The lack of official strategic documents in the field of cyber red teaming may be a result of several factors. First, since most nations are still in the early phases of developing extensive military cyber capabilities, developing a separate framework for cyber red teaming may not be among the main priorities. Additionally, even if (cyber) red teaming is taking place, it may be organised sporadically or on an ad hoc basis.[35] Also, red teaming may be mostly used in artificial exercise environments, and developing a separate framework or a doctrine may therefore be unnecessary. Another reason behind the lack of doctrines and other framework documents could be a deliberate strategy that aims to maintain the existing 'unregulated' freedom to conduct red team operations.[36] This aspect might be even more relevant in the constantly evolving domain of cyber security.

Assembling the cyber red team

Independent of the level of ambition for a military cyber red team capability, any red team has to comprise a wide range of cyber security experts who can provide an adversarial or 'outside-the-box' view when conducting red team assessments.[37] The following section will focus on the questions of who could be performing the cyber red teaming and what are the likely obstacles dependent on the chosen policy for assembling the cyber red team.

There may be several problems in the recruitment process of a military cyber red team. First, the process can be constrained by the well-known issue of recruiting cyber security experts for the public sector, which often lacks the necessary resources to compete with private companies.[38] Even if sufficient resources are allocated, the rigid pay policies and the public perception of working for the military might still hinder the ability to accommodate the rising demand of cyber security experts.[39] A possible way to overcome these issues is to design 'cyber-specific' pay policies in order to be able to provide competitive salaries, and market the unique

---

[34] 'The Defence Cyber Strategy,' Ministry of Defence of the Netherlands, 2012, http://www.ccdcoe.org/strategies/Defence_Cyber_Strategy_NDL.pdf pp. 11.
[35] Matthew Lauder, 'Red Dawn: The Emergence of a Red Teaming Capability in the Canadian Forces,' *Canadian Army Journal*, Summer 2009, http://canadiandefence.com/wp-content/uploads/2012/10/Lauder_Red-Dawn-The-CF-and-Red-Teaming.pdf.
[36] Brendan Mulvaney, s*upra* note 28
[37] Luc Dandurand, 'Rationale and Blueprint for a Cyber Red Team Within NATO, an essential component of Alliance's Cyber Forces,' in Christian Czosseck, Emil Tyugu, Thomas Wingfield (Eds.), *2011 3rd International Conference on Cyber Conflict*, NATO CCDCOE Publications, Tallinn 2011.
[38] Read more in Martin C. Libicki, David Senty, Julia Pollak, *H4cker5 wanted: an examination of the cybersecurity labor market*, RAND Corporation, 2014, p. 8, http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf.
[39] *Ibid.*

attractive elements that are related to working within the military cyber red team.[40] Hiring specialists from the labour market may be inevitable in the context of cyber security and red teaming, but having a separate training capability for military red teaming can also be an option. For instance, there are examples of educational institutions in the US which have successfully contributed to the wider red team community such as the University of Foreign Military and Cultural Studies.[41] As cyber red teaming requires specific technical training in comparison to 'classical' red teaming, separate educational programmes would have to be established. Again this is a matter of available resources and the level of ambition over whether it is possible or reasonable for the military to compete with civilian educational organisations.[42]

There are a growing number of education providers around the world who prepare and deliver cyber red teaming training. Cyber security experts who deliver that training help military officers, governmental officials and private sector employees in this field. The SANS institute is one of the best-known reputable education and research organisations in the field with on site, on demand or self-study options.[43] Some of them also give examinations to certify individuals on the specific subject matter expertise for cyber red teaming. Another option would be preparing in-house training. In some cases this can be a better and preferred option, depending on budget constraints, for preparing cyber red teams for a special mission which must be kept confidential. In such cases, investing in training for military officers to be able to prepare cyber red teaming training might have beneficial outcomes in the future. However, given the specificity of career management in the military, the training must be done according to the needs of the organisation. In military communities, there is significant staff turnover which can mean a loss of competences to a certain extent. In the case of cyber red teaming that has to be taken into account, especially when the cost of training is so high.

Since cyber security encompasses a broad spectrum of more specific fields which all require different skill-sets, and if 'full-spectrum' cyber red teaming is the aim, the team has to be made up of professionals from very different areas of expertise. For example, the cyber red team may include ethical hackers or pentesters, network engineers, social media specialists or even psychologists.[44] Again, this depends on the resources, the level of ambition of the military and the planned scope of red

---

[40] *Ibid.* Also, see David Welna, 'What's The NSA Doing Now? Training More Cyberwarriors ,' *NPR*, http://www.npr.org/2014/04/30/307963996/whats-the-nsa-doing-now-training-more-cyber-warriors

[41] For example, see: Scott Swanson, 'Enhancing Red Team Performance: Driving Measurable Value and Quality Outcomes with Process Improvement', *Small Wars Journal*, 5 October 2012, http://smallwarsjournal.com/print/13333.

[42] For example, see: '2014 Best Schools for Cybersecurity', Ponemon Institute Research Report, February 2014, http://www.hp.com/hpinfo/newsroom/press_kits/2014/RSAConference2014/Ponemon_2014_Best_Schools_Report.pdf.

[43] Prices of the courses may vary from $2000 up to $6000 at SANS. http://www.sans.org/ondemand/courses/all.

[44] Zachary Fryer-Biggs, *supra* note 9

teaming activities. If 'holistic' cyber red teaming is not pursued or not possible due to limited resources, then the organisation might aim to assess a specific set of vulnerabilities. In this case, a smaller number of professionals with specific skill-sets would be required. Therefore, it may be a more feasible approach if a cyber red team is formed to assess only a certain type of vulnerability (e.g., if methods of social engineering would be successful in the targeted organisation).

Since a wide range of skillsets and an alternative viewpoint are essential for cyber red teaming, the need to involve specialists from the private sector is highly likely.[45] Likewise, involving the private sector could prove to be a more flexible and cost-efficient approach when the assessment of a specific range of possible vulnerabilities is sought. On the other hand, private sector involvement may entail some problems with regard to the willingness to share sensitive information. Since one of the critical aspects in red teaming is mimicking the adversary, implementing classified intelligence on the possible attack methods could be necessary.[46] Sharing intelligence might be problematic when private contractors are involved.[47] In addition, there is the question of whether the targeted organisations would allow themselves to be vulnerable and to reveal security flaws to third parties that are not from the military.

A noteworthy approach in the context of private-public cooperation in cyber red teaming is applied by the US NSA which is claimed to be hosting one of the most effective teams in the world.[48] It is reported that the NSA's red team, in addition to having members from the military, also employs people from the private sector with the restriction that the civilians and contractors play a supporting role, such as writing exploits, while the military personnel are tasked to conduct the actual operations.[49]

Another interesting and alternative view is provided by a proposal to have a NATO cyber red team to test and increase the cyber security of NATO's CIS by controlled but unannounced cyberattacks.[50] The proposal also mentioned the theoretical possibility of using NATO's red team to support NATO's members and partners. [51] The idea was put forward in 2011, but has not come to fruition since it would probably be difficult to achieve agreement among the Allies on such politically sensitive practices.

---

[45] Scott Applegate, *supra* note 26
[46] Zachary Fryer-Biggs, *supra* note 9
[47] *Ibid.*
[48] Glenn Derene, 'Inside NSA Red Team Secret Ops With Government's Top Hackers,' Popular Mechanics, 30 June 2008, http://www.popularmechanics.com/technology/how-to/computer-security/4270420
[49] *Ibid.*
[50] Luc Dandurand, *supra* note 37
[51] 'A proposed Cyber red Team (CRT) has been under discussion since a number of years. The CRT is intended to conduct penetration testing of NATO's own systems, but could theoretically be employed to support NATO members and partners.' In Alexander Klimburg (Ed.), *National Cyber Security Framework Manual*, NATO CCDCOE Publication, Tallinn, 2012, p. 183.

While discussing the possible formation of a NATO cyber red team, Luc Dandurand provided an example of the organisational structure of a cyber red team (see Figure 2); the specific size and assembly of a red team would, of course, depend on several factors such as the aims and available resources of the organisation.[52]

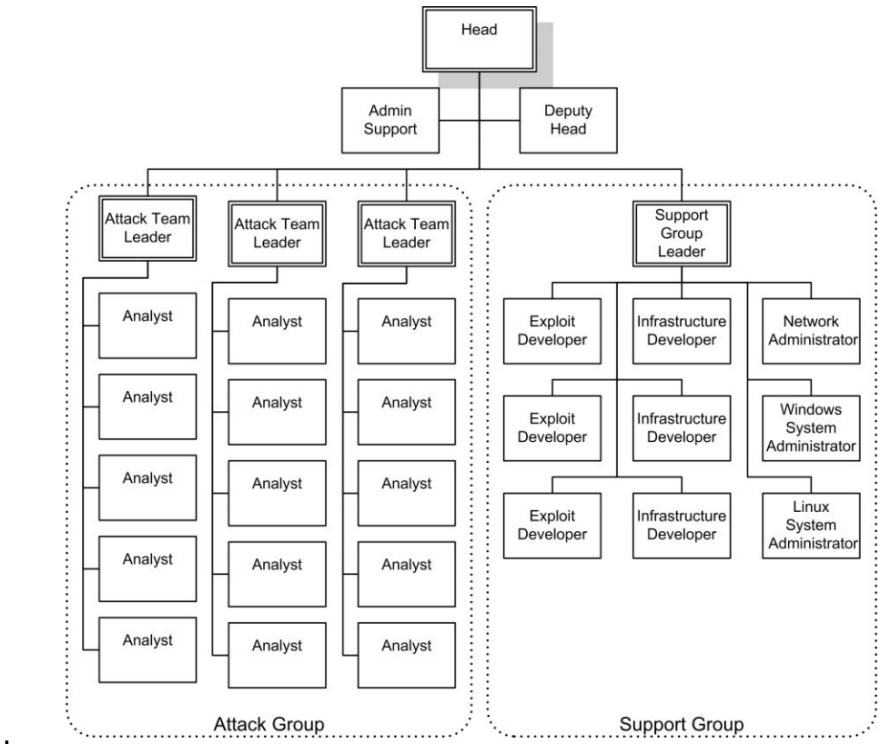

Figure 2 – Example of a cyber red team's organisational structure

Skill requirements for cyber red teams

Essentially, cyber red teams focus on 'how systems fail' instead of 'how systems work'. Starting from the outermost layer, which is the reconnaissance phase, to the innermost layer, exfiltration of system targets, cyber red teams try to find vulnerabilities in systems, be it in a technological system or a human operator, and exploit them. This requires specific skill sets.

There are a variety of educational options to improve competences in order to successfully accomplish cyber red teaming missions. Zero-day exploits, also known as *zero-days*, are one of the most important tools for both cyber red teaming operations and black hat hacking.[53] Exploring the vulnerabilities in computer

[52] Luc Dandurand, *supra* note 37
[53] Bilge, Leyla, and Tudor Dumitras. 'Before we knew it: an empirical study of zero-day attacks in the real world.' Proceedings of the 2012 ACM conference on Computer and communications security. ACM, 2012.

applications, usually it Operating Systems or Internet Browsers, and then writing an exploit code to leverage the attacks is a challenging task but once successfully accomplished, this exploit-program can be very powerful in gaining advantage, simply because the likelihood of getting caught by Intrusion Detection Systems (IDS) or by Intrusion Prevention Systems (IPS) is very low. Exploit development is therefore a precious skill. If any cyber red team has a member who possesses such capabilities, their horizon widens significantly and the quality of their work is improved thereby.

Writing an exploit code from scratch, or even finding it from publicly available sources,[54] is an important first step. But delivering those exploits is another important task for cyber red teams. The categorisation by different interest areas is generally as follows; network attacks, client side attacks and application attacks.

In network attacks, cyber red teams focus on networking operations such as scanning the network, mapping the machines and Local Area Networks (LAN), listing the IP addresses of available machines, and finding out which services are up and running. For other interest areas, network attacks play a huge role because the reports they produce would point the weakest entities in the network. This information would be further used during the exploitation for client side attacks or application attacks.

Client Side (CS) attacks deal with client computers which victims control. Since the Windows Operating Systems are very common, most exploitation efforts are spent against Windows machines in cyber red teaming. For the application attacks, however, there are different tools and applications as well, such as web and databases. Application attacks also receive a lot of attention from red teamers, firstly because web vulnerabilities are the ones which are facing to the entire world, and most of the time it is the very first step which the adversary takes. Database operations are also important, because most data warehouses store their operational data in a variety of databases within that organisation.

Other than technical skills, cyber red teams also require some social skills. Being a team player, having advanced communication skills with other team members, being fair and honest, and showing empathy to others are some of them. Other than team-related social factors, some skills which could be used during a cyber red teaming operation are also beneficial. Social engineering (in its IT rather than political sense) skill is one them. The ability to convince others via email or phone call can be very useful during the reconnaissance phase of the attack cycle. Also, it is a necessity for all cyber red team members to have a ‘thinking outside of the box’ mind-set. Most of the time, team players face a problematic issue or an obstacle during an operation.

[54] The Exploit Database, http://www.exploit-db.com.

Combining different exploits, forcing victims to make a mistake and taking advantage of their mistakes can be done if the attacker is innovative enough. As David Fulghum puts it 'officials concede the need for a better, earlier, screening system to identify the right people to become cyberwarriors. […] The intellectually arrogant, lone-ranger hacker is not the gold standard for innovative, multi-faceted cyberoperations'.[55]

Making cyber red teaming valuable & mitigating the risks

It is widely accepted that the main value of cyber red teaming and penetration testing lies in gaining knowledge on which cyber security measures work with the aim of improving the security posture of the targeted organisation. Nevertheless, there are cyber security experts who fundamentally question the value of some penetration testing practices.[56] One of the arguments against the activity is the assumption that, due to the 'inherently unsecure' nature of cyber security, a thorough penetration test will *always* prove that the client's networks are vulnerable, making the mere activity therefore impractical.[57] Furthermore, 'effective' penetration tests could in some cases result in a report that indicates a 'discouragingly' high number of vulnerabilities that are not prioritised and cannot be all fixed due to limited resources.[58] Additionally, penetration tests can be associated with the risk of damaging the targeted networks.[59] Taking these factors into account, the value of the often expensive[60] penetration tests are put under question. It is therefore relevant to ask how penetration tests or cyber red teaming activities can produce added value for the targeted organisation.

As a first step to avoid a report that will result in an 'unrealistic' or 'overwhelming' list of suggestions, there is the option to limit the red teaming activity to test a certain area of vulnerabilities based on commonly exploited critical vulnerabilities,[61] although while essential, it would not serve the purpose of a red team. The cyber red team has to take the particular characteristics of the target organisation into account, implement an adversarial viewpoint by grounding its activities on the most probable attack methods. If this is achieved, the assessment would produce a report with a prioritised list of vulnerabilities, providing the targeted organisation a practical and cost-effective assessment.

---

[55] David Fulghum, 'Solitary Genius Trumped by the Socially Adept: The 'lone wolf' cannot compete against integrated cyberteams', *Aviation Week*, http://aviationweek.com/awin/solitary-genius-trumped-socially-adept.
[56] For example, see Bruce Schneier, 'Is Penetration Testing Worth It?' *Schneier on Security* blog, 15 May 2007, https://www.schneier.com/blog/archives/2007/05/is_penetration.html.
[57] *Ibid.*
[58] Zachary Fryer-Biggs, *supra* note 9
[59] Luc Dandurand, *supra* note 37
[60] Scott Applegate, *supra* note 26
[61] Bruce Schneier, 'Is Penetration Testing Worth It?' Schneier on Security blog, 15 May 2007, https://www.schneier.com/blog/archives/2007/05/is_penetration.html.

Another factor to be highlighted in red teaming activities is the importance of having an expedient after-action report.[62] Simply put, the cyber red team's more 'compelling' activities during preparation, intelligence gathering and the exploitation phase may receive the most attention by the red teamers, and the 'less attractive', but arguably most relevant phase –reporting – receives less attention. One option to make sure that the red team focuses thoroughly on the after-action report is to have rigid methodology and standards for reporting in place.[63] Even if the report properly indicates the vulnerabilities, there is the question of how and whether the security threats are addressed. Problems may arise due to the lack of competence in the target entity. To that end, it is proposed that it would be an effective way to involve the red team in also implementing the defensive strategies.[64]

Even if the assumption that a penetration test is not particularly effective in securing networks holds true, there are other positive effects to be taken into account. Firstly, red teaming can provide a way to use a military's offensive capabilities: offensive capabilities could be applied to test the defence of networks, while cyber red teaming may provide an opportunity to develop and test these offensive methods.[65] In this context, it is questionable whether the aim of implementing an alternative or adversarial viewpoint can be achieved through using the military's own capabilities to conduct red team activities. Using only in-house entities might be counter-productive and produce compliance – a cyber red team, comprising only experts from a similar environment as the target, may already be aware of the main vulnerabilities in the target's networks and might not be able to take the much-needed 'outside-the-box' approach. In addition, especially in the context of exercise environments, using advanced offensive methods just for red teaming purposes can run the risk of revealing information on classified and sophisticated techniques to unwanted parties. However, using the military's offensive capabilities in red teaming can be preferred since it can be more cost-effective, and involving only military staff would avoid the security concerns that rise when private sector involvement is considered.

In addition to just testing the information networks of a specified target, red team assessments can also create value in a broader context by testing the 'human security' factor; whether the staff's response and procedures in the organisation are

---

[62] Scott Applegate, *supra* note 26
[63] *Ibid*. See also, for example, best practices outlined by such organisation as the SANS institute http://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343.
[64] Zachary Fryer-Biggs, *supra* note 9
[65] See General Keith B. Alexander's comments: 'U.S. Cyber Command: Organising for Cyberspace Operations,' House hearing before the Committee on Armed Services, 111 Congress, held 23 September 2010, http://www.gpo.gov/fdsys/pkg/CHRG-111hhrg62397/html/CHRG-111hhrg62397.htm.

adequate.[66] This also relates with the demonstrational value of red teaming; a real-life presentation of security flaws may result in an increase in awareness that will both educate the members of the organisation and legitimate investments in cyber security.

The value of penetration tests also comes into question when one considers the risk of having unintended negative effects on the target organisation's networks (e.g., the test may result in a denial of service or a loss of sensitive data). There are several factors which can be taken into account to mitigate this risk. As a very basic procedural first step before conducting any cyber red teaming activities is to sign a detailed contract between the cyber red team and the client organisation. The contract should include a clearly defined scope of authorised activities, and cover the liabilities and non-disclosure clauses.[67] Mitigating risks by setting a scope of activities is perhaps unavoidable, but it has to be taken into account that if the cyber red team is supposed to provide a truly 'uninfluenced' alternative view. Very precise limitations may be counter-productive.

Procedures to lower the risk of the red team's staff members acting maliciously and abusing their access should also be considered. For example, the 'two-person rule' is a possible method to establish a control mechanism during the red team's operations. In short, the members of the red team would be allowed to work only in pairs in order to confirm and control the actions conducted during the test.[68] Establishing a certain 'cultural' environment such as adhering to the rules of ethical hacking among the team is also important. There are other possible methods in this context, such as the requirement to test the exploit tools beforehand to anticipate possible negative 'side-effects' (e.g., using a sandbox).[69]

An aspect which is also worth elaborating on here is the 'cultural resistance' phenomenon. In essence, red teaming in the military can be viewed as something that points out faults and mistakes made by entities in the targeted organisation. This may result in discontent with the red team and a possible reluctance to accept that the activity be conducted.[70] If an outside entity – a contractor – is involved in revealing the vulnerabilities, the possible tensions between the military organisations can be lowered. Another proposed method to minimise internal tensions is to have

---

[66] For example, see: (ISC)2 Government Advisory Board Executive Writers Bureau, 'Penetration testing: Pros and cons of attacking your own network,' *GCN*, 4 February 2013, http://gcn.com/articles/2013/02/04/pros-cons-penetration-testing.aspx.

[67] For example, the contract could include a 'Sanctioned Targets List', see more in Luc Dandurand, 'Rationale and Blueprint for a Cyber Red Team Within NATO, an essential component of Alliance's Cyber Forces,' Christian Czosseck, Emil Tyugu, Thomas Wingfield (Eds.), *2011 3rd International Conference on Cyber Conflict*, NATO CCDCOE Publications, Tallinn 2011.

[68] *Ibid.*

[69] *Ibid.*

[70] Scott Applegate, *supra* note 26

the red team members assigned *ad hoc*, instead of having personnel who are doing red teaming as a full-time occupation.[71] In that respect, the role of the chain of command is central in order to alleviate potential tension.

It is apparent that the development or use of military cyber red teaming capabilities can be accompanied by a very wide range of different aspects to be taken into account in the context of policy and organisational requirements. More specific technical and legal considerations will be analysed in the following chapters.

[71] Scott Swanson, 'Enhancing Red Team Performance: Driving Measurable Value and Quality Outcomes with Process Improvement', Small Wars Journal, 5 October 2012, http://smallwarsjournal.com/print/13333.

3. Technical considerations for cyber red teaming activities

Cyber red teaming operations can help hedge against surprises. They do so by providing a wider and deeper understanding of potential adversary options and behaviour that can expose vulnerabilities in the strategies, postures, plans, programs, and concepts.[72] The organisational and policy considerations of cyber red teams were detailed in the previous section and there is a need to understand how the concept of cyber red teaming can be implemented from the technical standpoint.

Technical attributes such as design, development and execution are at the centre of the framework development for cyber red teaming activities. Since it relies heavily on technical opportunities available in the world of cyber, this section elaborates in two sections; infrastructure design and operational environment and execution.

The first part discusses the required environment, and what else is needed in order to deploy a cyber red teaming environment successfully. The second part defines the execution of cyber red teaming by explaining the defence in depth architecture of information systems, attack phases, and the tools and objectives which are commonly cited by cyber red teamers in an operation.

Infrastructure Design and Operational Environment

Cyber red teaming operations can be conducted in different environments, though there are two main options. The first is the actual operational environment, in other words, the 'Production Environment' from a system administration point of view. The second consists of specialised infrastructure, called 'Cyber Ranges'.[73]

a. 'Operational Environment'

The main goal of cyber red teams is to look from an adversarial perspective and explore potential vulnerabilities in the systems. While testing Information Technology (IT) systems the objective is to find weaknesses in the environment. If there is no additional setup or deployment, and if cyber red teamers use the current environment which they are trying to protect as a mission, then this means they are operating in the 'Operational Environment'.

This is where the *penetration testing* happens, against the team's own systems. Like adversaries, starting from the outer layer of the network, every exploitation and

[72] *Defense Science Board Task Force on The Role and Status of DoD Red Teaming Activities*. Office of the Under Secretary of Defense For Acquisition, Technology, and Logistics, Washington, D.C. 20301-3140, September 2003.
[73] Wihl, Lloyd, and Maneesh Varshney. 'A virtual Cyber Range for cyber warfare analysis and training.' *The Interservice/Industry Training, Simulation & Education Conference (I/ITSEC)*. Vol. 2012. No. 1. National Training Systems Association, 2012.

misuse of computer systems is intended to reach the most protected computers, servers and data. In military environments, there might be different confidentiality network layers in Operational environments, from top secret to unclassified, and it is possible to divide the networks and other computer systems depending on confidentially levels. In such cases, cyber red teams can work with each layer individually, or they can focus on leakage risks between layers. From a technical point of view, each confidentially layer might use similar technical environment, nevertheless, the exposed risks might differ since the asset value changes between each of them.

There are many benefits to this technique since the results of the test provide the same picture which attackers would achieve.[74] Penetration tests can only show what was possible during the period of the test, in that very time frame by the red teamers who have conducted it, and it is always possible that circumstances may evolve; the capabilities of the individuals in the cyber red team may vary, software or hardware updates in the target systems might occur, or merely luck effect may come into play. Many cyber security experts discuss the value of penetration testing however system owners can have fruitful results from penetration tests which support other auditing reports and vulnerability assessments.

Looking from the red teamers' perspective, there is much more. Targeting the operational environment is one of the easiest ways to hone technical skills, since it is their own environment. No additional setup or system deployment is necessary as it is in Cyber Ranges. Just plugging in the attacker laptop, such as a pre-prepared Operating Systems like Kali,[75] is enough to start testing, technically.

The operational environment might also require some thorough preparation, depending on the case. One of the reasons why such arrangements should be done beforehand is the possible damage that might occur from cyber red teaming actions. There are many harsh exploitation techniques which can take down a system, rather than getting a shell from the remote computer.[76] In fact, this is how exploitation works.

Taking buffer overflow exploitation as an example, if there is an anomaly within the program and if the attacker manages to send the malicious commands by overwriting the memory location and force the program to read the payload which the attacker has crafted, he might be able to leverage a successful exploitation which can result

---

[74] Allen, Lee. *Advanced Penetration Testing for Highly-Secured Environments: The Ultimate Security Guide.* Packt Publishing Ltd, 2012.
[75] https://www.kali.org/.
[76] As an example, multiple vulnerabilities in Ruby may lead to a denial of service (DoS) condition or allow execution of arbitrary code.Ruby Arbitrary code execution vulnerabilities: https://www.ruby-lang.org/en/news/2008/06/20/arbitrary-code-execution-vulnerabilities/.

with a reverse shell being sent back to the attacker's computer. It is clear that, during the exploitation phase, attackers force the program to crash but in a way where they can send their malicious commands. After successfully exploiting the application, they can also terminate the program or let it continue to work normally. If something goes wrong and the exploit fails, it is likely that the program will fail as well, which could result in a Denial of Service (DoS). If the exploit has targeted the Kernel Level Vulnerabilities, the end result could cause more dramatic problems such as crashing the Operating System. Higher level privilege-seeking exploits are more valuable, but if they fail, catastrophic consequences might result. There are also other direct exploits which are designed to result in a DoS. If they are executed in operational environments requiring constant availability such as airspace surveillance there will be a need for actions which do not create disruptions that would lead to loss of service. In such a case, a military organisation could not afford to take such risks.

Although there is no single solution for such issues, there are a couple of options available. The first is to create backups just before cyber red team testing operations. These backups would prevent loss of data and availability issues which might occur during or after the test. Another very common mechanism to prevent problematic consequences would be using Virtual Environments, particularly with the proliferation of cloud technologies, such as Virtual Private Servers (VPS). These virtual environments have also options for such cases, such as reverting the machine back to its original state, which would be very useful.

Cyber red teaming against the same operational environment is very powerful and can be very useful from both defensive and offensive perspectives. However, this approach also requires care due to the sensitive nature of production systems and other possible inconveniences that may be caused by the attacks conducted by the cyber red teams.

b. Cyber Ranges

Cyber Ranges constitute the second type of operational environment for cyber red teams. Operational Environment deals with red teaming actions against the very same production domain which every server, computer, network and storage devices reside. By contrast Cyber Ranges are simulated environments where red teams can mimic adversarial actions and execute attacks. This approach is particularly valuable for military organisations.

The main reason behind the deployment of Cyber Ranges is testing and evaluating cyberspace concepts, policies, and technologies.[77]. The aim of the effort is similar to the deployment on Operational Environment, but for Cyber Ranges all the

[77] *Department of Defense Strategy for Operating in Cyberspace* (2011), US DoD

technology, infrastructure and test-beds are specifically crafted in virtual networking environments.[78]

There are different ways of designing a Cyber Range depending on the ultimate goal; penetration testing of specific hardware or software, creating a training environment, benchmarking and validation of a technology, and cyber exercises between red and blue teams are the most common. This section will focus on red vs. blue team exercises since they are very popular and since the idea behind them reflects red teaming operations.

Simulated environment is the backbone of Cyber Ranges, including red vs. blue cyber exercises. It contains many infrastructural elements such as routing devices, networking devices, storage devices, red team (attacker) and blue team (target) systems including all the client machines and servers, supporting systems, traffic generators, the simulation (green) team's own systems, automatic availability, and scoring systems and visualisation systems.

As an example of the hardware requirements; networking devices, firewalls, VPN concentrators, switches, storage devices, blade chassis, virtual machine host services and hardware-based IDS/IPS devices might all be required. For the software requirements, in order to simplify the list we can take a closer look at Locked Shields 2014.[79] Different versions of operating systems like Windows and Linux, web servers, databases, mail servers, file server applications, software repositories, monitoring tools and VOIP software, collaboration environments and Virtual Lab Managers were all needed.

Very similar to simulated environments, 'Reference Systems' can also be used in the context of Cyber Ranges. Reference Systems are configured in a similar manner as operational environments the only major difference being the fact that there is no real data in the Reference System. The idea is very helpful to test the hardware and software of the system, without risking any data leakage as it might be sensitive to play with the inherent architecture of a novel system even though it contains no operational information.

Another example of a successful Cyber Range implementation could be a Cyber Defence Exercise (CDX), which is organised by the NSA for military academy cadets from the US and Canada, to create an opportunity for learning and experiencing

[78] Leblanc, Sylvain P., et al. 'An overview of cyber attack and computer network operations simulation.' *Proceedings of the 2011 Military Modelling & Simulation Symposium*. Society for Computer Simulation International, 2011.
[79] Locked Shields 2014 After Action Report, https://ccdcoe.org/sites/default/files/documents/LS14_After_Action_Report_Executive_Summary.pdf.

cyber threats in a virtualised environment.[80] From one of the previous iterations of CDX, a network layout for that Cyber Range was published.[81]

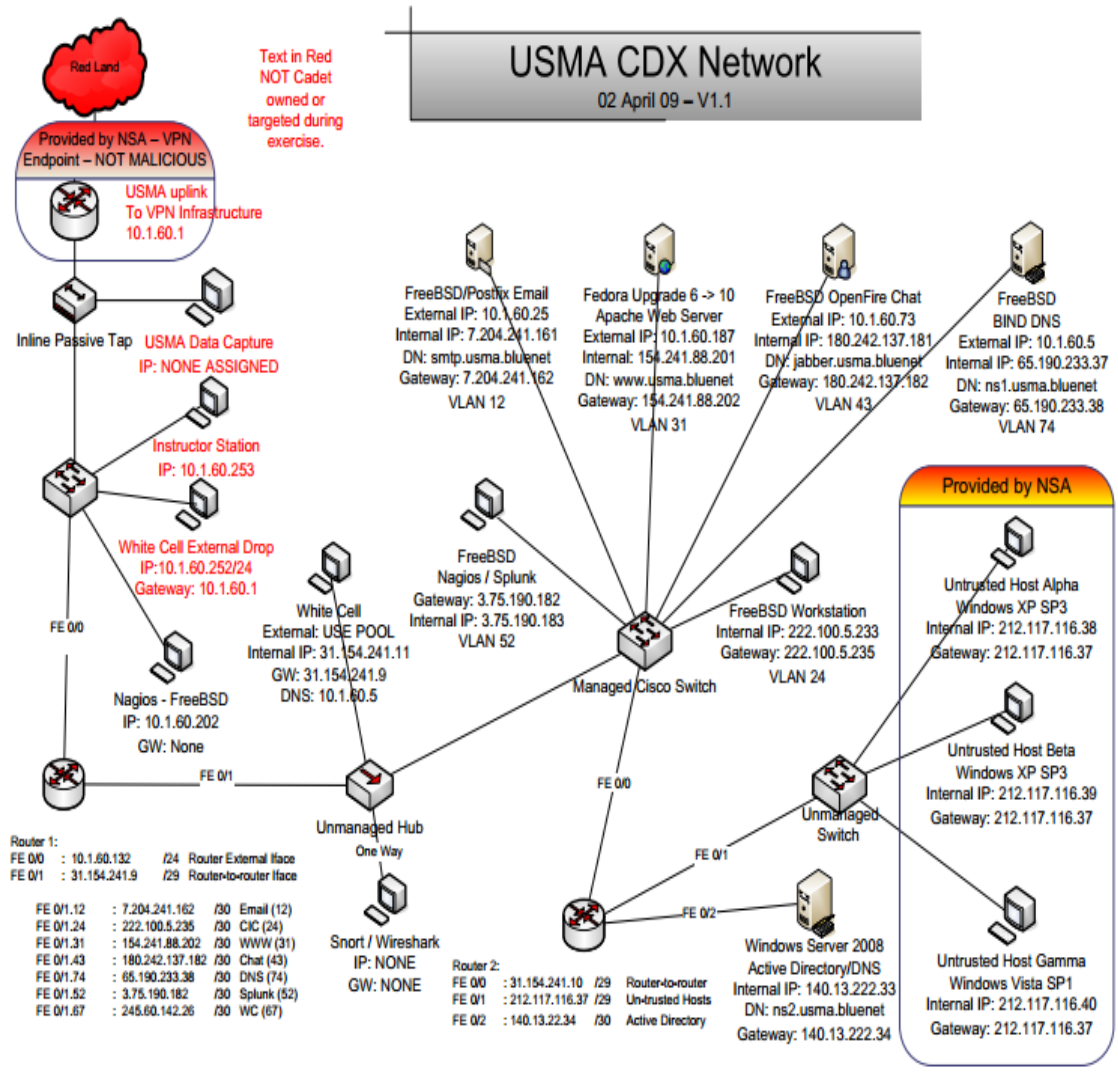

Diagram 3USMA CDX Network Layout used in a CDX Cyber Range

The Estonian Defence Forces have also invested in developing Cyber Range capabilities during recent years. One of the outcomes of this effort was observed during the NATO Cyber Coalition exercise,[82] since this Cyber Range was used effectively. Such technical capabilities help foster better and stronger relationships

[80] U.S. Military Academy Wins NSAs 14th Annual Cyber Defense Exercise, https://www.nsa.gov/public_info/press_room/2014/u_s_military_academy_wins_nsas_14th_annual.shtml.
[81] USMA CDX Network, http://www.westpoint.edu/crc/SiteAssets/SitePages/DataSets/CDX_2009_Network_USMA.pdf.
[82] Largest ever NATO cyber defence exercise gets underway, http://www.nato.int/cps/en/natohq/news_114902.htm

within allies. NATO Supreme Allied Commander for Transformation (SACT), French Air Force General Jean-Paul Paloméros, stated that this capability will allow NATO 'to conduct cyber-related training, exercises, and education [...] in a trusted and secure environment' and 'will provide an essential contribution to our effort to build more responsive and flexible forces, adapted to a very challenging security environment, which we are addressing during the Wales Summit'.[83]

Though necessary for cyber red teaming activities, these infrastructures come at a certain cost whether it is for their set-up or their maintenance.[84] A virtualised environment is the key infrastructural requirement in Cyber Ranges. Those exercises are not played on servers used for day-to-day business operations; rather, they are created individually for a specific mission. All the data, software and hardware can be different from the actual ones. There are various intentions behind this approach: Reflecting the vulnerable systems without worrying about being hacked by real adversaries, hiding the real operational environment from the players, creating a logical scenario which could be followed with a step by step exploitation in order to compromise everything, and so on. One of the key important factors for this implementation is to get maximum benefit from the exercise. Red teaming operations could play a vital role here, since they can train the blue teams for latest attacks, or they can try to improve their attacking skills in this environment. No matter which part the red teamers are playing, there is an important task for them.

There are also some disadvantages to Cyber Ranges. First and foremost, Cyber Ranges are not real operational environments; they try to reflect all or part of the possibilities which adversaries could use. Including all vulnerabilities is a daunting task, if possible at all. Designing, developing and deploying the systems for a Cyber Range is another issue, since it requires lots of time and effort. Cyber Ranges constitute an important terrain for cyber red teams, however, the success rate totally depends on the design and deployment elements during preparation.

Execution: putting the cyber red team into play

Execution of attacks is the last part to be covered in this section, yet it is the core of cyber red teaming operations. Different concepts and layers will be discussed, starting from the defence in depth concept and attack phases, to available tools and objectives for cyber red teams.

---

[83] SACT and the Estonian Minister of Defence sign an agreement to establish the NATO Cyber Range Capability, http://www.act.nato.int/sact-and-the-estonian-minister-of-defence-sign-an-agreement-to-establish-the-nato-cyber-range-capability.

[84] On that note, see the contract awarded to Lockheed Martin Corporation to support the NCR for $82.5 million https://www.fbo.gov/utils/view?id=734fb00c551305f3af35786f86379610.

a. Defence in Depth

The concept of defence in depth is not solely based on cyber security matters. Rather, it is a strategy of fundamental principles to protect the assets of an organisation.[85] In the cyber context, defence in depth also involves discussion of how to protect in every possible way the data and the information. It is about not trusting any layer and placing additional mechanisms, assuming that each layer could fail at some point. When these layers are combined, the possibility of infiltration decreases significantly.[86]

As the National Security Agency (NSA) sees it, adversaries can attack a target from multiple points using either insiders or outsiders, and thus an organisation needs to deploy protection mechanisms at multiple locations to resist all such attacks.[87] There are different focus areas where cyber red teams would face when attacking, such as network boundaries, enclave boundaries, computing environment and applications (see Figure 4).

Cyber red teams deal with different challenges at each layer. There might be serious vulnerabilities in inner layers, such as application vulnerabilities, but if it is not possible to bypass network perimeter security devices, it might not be possible to get in. Likewise, if the network boundaries are not protected adequately but there is no application level vulnerability or configuration mistakes, this would also end with no results. This is why cyber red teams should encompass different types of expertise to deal with each layer by full extent.

a. Attack Flow

The red team cycle was described as having the following steps; preparation, reconnaissance, execution, after-action and analysis phases. Although this is valid for cyber red teaming operations, there are different approaches, especially regarding the technical aspects of the attack itself.

Advanced cyberattacks which cyber red teams conduct do not involve a single discrete event. Rather, they take several steps to accomplish the mission.[88] There is a particularly useful framework on this approach, which is called the cyber kill-chain.[89] According to that analysis, cyber red teams divide the tasks into distinct

---

[85] Clifton L Smith, 'Understanding concepts in the defence in depth strategy.' *Security Technology, 2003. Proceedings. IEEE 37th Annual 2003 International Carnahan Conference on*. IEEE, 2003.
[86] Chris Peake, 'Red teaming: The art of ethical hacking.' *SANS Institute* (2003).
[87] Defense in Depth, *A practical strategy for achieving Information Assurance in today's highly networked environments*, https://www.nsa.gov/ia/_files/support/defenseindepth.pdf.
[88] Lachow, Irving. *Active Cyber Defense: A Framework for Policymakers*. Center for a New American Security, 2013.
[89] This approach was originally presented by Eric M. Hutchins, Michael J. Cloppert and Rohan M. Amin, 'Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains' (paper presented at the 6th Annual International Conference on Information Warfare and Security,

actions which would result with taking over the target system, such as connecting to the remote system with exploits which follow different phases; *reconnaissance*, *weaponisation*, *delivery*, *exploitation*, *installation*, *command and control*, and *action* phases.

Figure 3– Cyber Kill Chain Model[90]

Reconnaissance is the first phase which deals with identifying and selecting the target. *Weaponisation* is the preparation phase for exploit development, whereas *delivery* is the first phase which the attacker makes contact with the victim for the first time and sends the already-developed exploit.

The *Exploitation* phase contains the actions from victims, such as trigging the exploit by opening the malicious content. Once exploited, the malware infects the system and tries to hide itself from monitoring solutions like IDS in the *installation* phase. In the *command and control* phase, the malware talks back to home and send-receive updates if necessary. In the last phase, the cyber red teams send commands to accomplish a task, such as taking down the system or accessing sensitive data at remote computers.

Washington, March 17-18, 2011), http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf.

[90] Figure taken from Irving Lachow, Center for a new American Security, Active Cyber Defence – A framework for policy makers: http://www.cnas.org/files/documents/publications/CNAS_ActiveCyberDefense_Lachow_0.pdf .

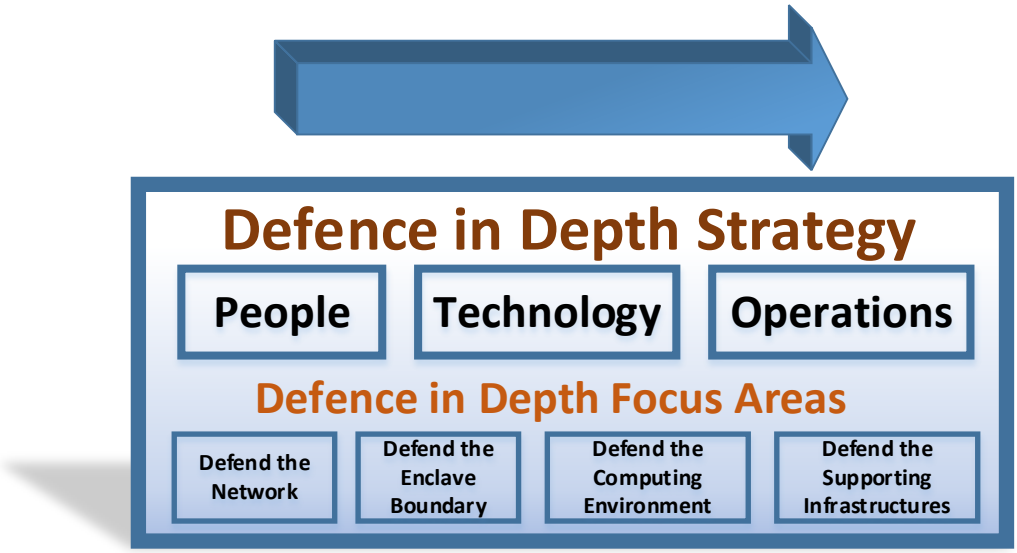

Figure 4– Focus Areas and Defence in Depth Strategy

b. Tools

The execution of cyberattacks and all the actions which cyber red teams carry out require an available set of tools. For the steps discussed above (the *cyber kill chain* or *cyber red teaming cycle)* members of cyber red teams need tools to write the exploit codes, deliver them and cleaning them, if necessary.

There is a wide variety of options for cyber red teaming tools, both open-source and licensed. Although it is very popular to write a new tool and share it with the cyber security community nowadays, there are also very popular frameworks like *Metasploit* which extensively cover many tools, payloads and exploits.[91]

Different portals and cyber security related webpages share the most commonly used tools list.[92,93] They vary depending on the level of interaction and the phase of cyber red teaming operations. Some tools are very capable and can be useful for the entire campaign.[94] Others are specialised for a specific task, such as detecting and exploiting wireless networks (wardriving).[95]

For military cyber red teams, there are caveats about using both licensed and open-source tools. Since most operations are sensitive in nature, executing licensed tools without knowing exactly what they are doing or how they are behaving in certain

[91] Metasploit: Penetration testing software, http://www.metasploit.com.
[92] Top 20 Penetration Testing Tools, http://www.softwaretestinghelp.com/penetration-testing-tools.
[93] SecTools.Org: Top 125 Network Security Tools, http://sectools.org.
[94] Kali Linux Distribution is an example, although it is not a tool by itself, rather, a collection of most frequently used tools in cyber red teaming. http://www.kali.org.
[95] Kismet, http://www.kismetwireless.net.

conditions could be unwise. Since the source is not open, red teamers would not know the inherent details of such applications.

Open-source tools might also have issues if, for instance, the publisher is not trusted and the source code is not reviewed before using the tool. There are some scripts on the internet which claim to execute a specific exploit, but it turns out they are opening a reverse-shell back to the author’s computer, or even wiping the user’s hard drive as a very bad joke. This is one of the reasons why cyber red teams should only use tools from trusted sources and focus on developing their own tools in this field. This would also give flexibility to the cyber red teams to tailor their needs and reflect them into their very own in-house applications.

To perform efficiently, cyber red teams require a specific technical environment as well as tools that can be used to assess the vulnerabilities of the system. In order to complement this framework, legal considerations shall be looked on in the next section.

4. The legal implications of cyber red teaming activities

Cyber red team activities can be subject to a certain number of legal barriers and requirements that will be described in the first section. We will describe how these activities can be legitimised and thus authorised through legal provisions. Having these rules in mind, we will detail the legal risks to which these specific activities can be exposed. The legal risks described and commented on here are not specific to cyber red teaming but are common when engaging in cyber activities.

Legal framework for the use of cyber red teams

Cyber security is an obligation for most information systems operators, and failing to meet the requirements places the person in charge of their security in a difficult position. There is also much debate as whether or not the regulations in place can render cyber red teaming activities lawful. Some concerns have arisen and there is a necessity for a clear legal framework enabling these activities.

Cyber red teams should be able to perform certain types of operations that would otherwise be considered as criminal offences according to national law. Actions carried out against an information system in order to assess its vulnerability such as hacking into a system and modifying or retrieving data could constitute a computer offence as described in the Convention on Cybercrime.[96] For example, hacking into a computer system would be qualified as illegal access, as defined in Article 2 of the Convention. This document provides for a thorough harmonisation of criminal law regarding cyberattacks, but also gives some hints as to what could constitute a 'good' cyberattack in the case of cyber red teaming activities.

The notion of intent is the cornerstone for determining whether a computer action is legal or illegal and surely these vulnerability assessments are quite clearly based on a legitimate concern . The expression used in the convention on Cybercrime is 'without right'. According to its explanatory report, 'it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defences, excuses, justifications or relevant principles under domestic law'.[97] The European Directive on computer attacks adopted on 12 August 2013, and to be incorporated into national laws by September 2015, has also posed the principle of

[96] Convention on Cybercrime, Budapest, 23 November 2001. http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm The convention has been ratified by 44 countries. Among NATO members states, only Canada, Greece, Poland and Turkey have not ratified the Convention but all of them have signed it, see http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

[97] Point 38 of the explanatory report of the Convention on Cybercrime, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

intent and considers that, in cases of 'mandated testing or protection of information systems', any criminal intent can be excluded.[98]

The performance of cyber red teaming activities may be subject to certain limitations and the case of the possession or creation of malware is very relevant when discussing the issue of the lawfulness of cyber red teaming. The Convention on Cybercrime imposes a general ban on the misuse of devices; to commit a criminal offence, one needs certain means ('hacker tools') and that it is therefore illegal to use certain devices and programs. Thus, Article 6 of the Convention states that:

when committed intentionally and without right:

a. the production, sale, procurement for use, import, distribution or otherwise making available of:
   i. a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with Articles 2 through 5;

   ii. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b. the possession of an item referred to in paragraphs a. i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.'

However, this article does not impose criminal liability when these devices including computer programs are used for the authorised testing or protection of a computer system.[99] The French Criminal Code was amended to include a conforming provision. Even though the case for the possession of malware for security testing seems to be relatively clear, there are still concerns among certain security professionals as shown in a survey conducted by the European Union Network Information Security Agency (ENISA), especially regarding the lawfulness of the use

[98] Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, Recital 17: 'This Directive does not impose criminal liability where the objective criteria of the offences laid down in this Directive are met but the acts are committed without criminal intent, for instance where a person does not know that access was unauthorised or in the case of mandated testing or protection of information systems, such as where a person is assigned by a company or vendor to test the strength of its security system.' http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF.

[99] Paragraph 2 [of article 6 of the Convention on Cybercrime] sets out clearly that those tools created for the authorised testing or the protection of a computer system are not covered by the provision. This concept is already contained in the expression 'without right'. For example, test-devices ('cracking-devices') and network analysis devices designed by industry to control the reliability of their information technology products or to test system security are produced for legitimate purposes, and would be considered to be 'with right'.

of tools in their daily activities.[100,101] Nevertheless, there are no reports of any prosecution following the performance of such activities and it seems as though this concern is over exaggerated.

Overall, these specific regulations recognise the use of security testing and audits as perfectly lawful as their intent is built on a legitimate concern. Building up the case for cyber red teaming requires that these activities are considered as part of a sound and lawful cybersecurity policy.

Cyber security can be a legal notion in national public law and it is often the case that the security of one's information systems is a legal obligation. Deriving from national cybersecurity strategies, a number of national regulations contain provisions which state that information systems need to be secure[102] and the manner in which they are worded would require the performance of penetration testing, and hence cyber red team activities.

In addition to the specific cyber security regulations that can be found, there are general obligations in other bodies of law requiring that an operator's information system is secure. These regulations clarify the lawfulness of the use of cyber red teams for security purposes. For example, banking regulations in European countries clearly specify these obligations.[103][104] Similarly, the European Union directive regarding the protection of personal data also imposes this obligation. Not only does it formally state the obligation for security for information systems processing

[100] European Union Network Information Security Agency.
[101] The Directive on attacks against information systems, A Good Practice Collection for CERTs on the Directive on attacks against information systems, ENISA P/28/12/TCD, Version: 1.5, 24 October, 2013.
[102] The Czech Republic, for example, mentions it in Chapter 2 of its Cyber Security Act draft: 'Security measures mean a complex of activities, with the purpose of ensuring the security of information in information systems and availability and reliability of services and networks of electronic communications in cyber space'. In addition to that 'Public authorities and natural and legal persons […] are obliged in the extent necessary for ensuring cyber security to determine and implement security measures for critical information infrastructure information system, critical information infrastructure communication system or important information system and to keep security measures record in security documentation'. https://www.govcert.cz/download/nodeid-591/.
[103] Article 228, paragraph (h) of regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013R0575&from=EN.
[104] Article 533-2 of the French Banking and Monetary Code: 'The investment service providers operate on the basis of sound internal procedures, internal auditing capacities, efficient risk analysis processes and effective procedures for the control and safeguarding of information systems' (translation of the authors). http://www.legifrance.gouv.fr/affichCode.do;jsessionid=BAF2E3E74FB664655E23FD42EF8ADF66.tpdjo02v_1?idSectionTA=LEGISCTA000006170646&cidTexte=LEGITEXT000006072026&dateTexte=20141104. The German banking act does also contain a similar provision in its paragraph 24.c. section 6: 'The credit institution and BaFin shall put in place state-of-the-art measures to safeguard data protection and data security, which in particular shall guarantee the confidentiality and integrity of the retrieved and transmitted data. The state of the art shall be defined by BaFin in consultation with the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik) by a procedure of BaFin's choice.' http://www.bundesbank.de/Redaktion/DE/Downloads/Aufgaben/Bankenaufsicht/Gesetze_Verordnungen_Richtlinien/gesetz_ueber_das_kreditwesen_kwg.pdf?__blob=publicationFile

personal data, it also requires that the operators implement the necessary technical measures. [105]

Security incidents like the numerous breaches leading to involuntary disclosures of significant amounts of personal data have put a lot of pressure on stakeholders to make sure that a certain level of compliance to the security requirements is met, especially when concerning critical infrastructure information systems.[106,107] Increasingly drastic cyber security measures have the following corollary for the operator supposed to implement them; he must make sure that they work. Measures such as vulnerability assessments can be part of these duties. Regulations, in that regard are more demanding and force operators to perform audits on their own security systems. These provisions are now to be found in a number of NATO member states' laws and are relevant to the drafting of a legal framework for cyber red teaming.

The case of France is typical of the new policies that are being implemented. For example, to ascertain the level of security of critical infrastructure operators, are required to implement testing and audit measures within a defined timeframe.[108] These new provisions include the possibility of state entities performing these vulnerability assessments. The exact level of technical testing remains to be defined by the ANSSI (French national authority on the security of information systems)[109] which also set the security standards. In Germany, the BSI[110] (Federal Office for

---

[105] Article 17, paragraph 1 of the Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 'member states shall provide that the controller must implement appropriate technical and organisational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing',http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML

[106] 'Critical infrastructure' means an asset, system or part thereof located in member states which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions,' Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. In the United States, critical infrastructure is defined as 'systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.' Executive Order 13636, Improving Critical Infrastructure Cybersecurity, February 2013, http://www.nist.gov/cyberframework/.

[107] Martin Giles, 'Defending the digital frontier', *The Economist*, 12 July 2014 http://www.economist.com/news/special-report/21606416-companies-markets-and-countries-are-increasingly-under-attack-cyber-criminals.

[108] Article L. 1332-6-3 of the French Defence Code: 'At the request of the Prime Minister, [the operators of critical infrastructure] will submit their information systems to testing in order to assess the level of security and compliance with security rules defined in article L. 1332-6-1. These tests are performed by the National Information System Security Agency (ANSSI) or by state entities designated by the Prime Minister or by certified service providers' (Translation of the authors).

[109] Agence Nationale de Sécurité des Systèmes d'Information.

[110] Bundesamt für Sicherheit in der Informationstechnik.

Information Security) also concludes that it is necessary to 'undertake systematic assessments of critical areas of the company and facilities in cooperation with the authorities which are responsible for internal security […] in order to establish whether they may constitute a key target in principle, in view of which the possibility of the impairment, interference with or destruction of the facility concerned exists.'[111] The draft legislation that is currently being considered in Germany hints that similar measures will be taken.[112]

In the United States following the President's Executive Order 13886,[113] the NIST[114] framework[115] that was elaborated in 2014 does provide for the use of vulnerability assessment as one of the basic requirements to limiting risks. In European Union law, some basis for this obligation of cyber security can be found in the draft of the Network and Information Security Directive.[116] Article 14 of this draft Directive states that 'public administrations and market operators will take the appropriate technical and organisational measures to manage the risks posed to the security of the networks and information systems which they control and use in their operations'.[117] To a certain extent, this general obligation of cyber security made by states imposes a real standard of care for operators. [118]

The obligation of cybersecurity is provided for in a number of regulations but given their variety and their difference in scope, there is no 'one size fits all' requirement yet, except for the European directive project which outlines a standard of care for a number of operators. These technical operations may include the performance of cyber red team activities.

Authorisation to conduct vulnerability assessments is particularly important including the case of non-notified exercises. If a designated team is to be performing such tasks on military information systems and also on other information systems outside

---

[111] The German 'Baseline protection of Critical Infrastructures guide' provided by the BSI, p.29.
[112] Germany unveils draft cyber security law to protect 'critical infrastructure' http://www.out-law.com/en/articles/2014/august/germany-unveils-draft-cyber-security-law-to-protect-critical-infrastructure/.
[113] Executive Order 13636 of February 12, 2013, 'Improving Critical Infrastructure Cybersecurity', section 7 paragrah b), 'The Cybersecurity Framework shall provide a prioritised, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk'. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf
[114] National Institute for Standards and Technology.
[115] 'Improving Critical Infrastructure Cybersecurity Executive Order 13636 Preliminary Cybersecurity Framework', National Institute of Standards and Technology, p.27. http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf
[116] Project of directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union February 2013, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN
[117] *Ibid.*
[118] On that discussion see Scott Shackleford, Andrew Proia, Brenton Martell, and Amanda Craig 'Toward a Global Cybersecurity Standard of Care? Exploring the Implications of the 2014 NIST Cybersecurity Framework on shaping Reasonable National and International Cybersecurity Practices' forthcoming in the *Texas International Law Journal*.

of the military domain such as government systems or critical infrastructure networks, there is a clear need to clarify the liability and scope of the activities that may be undertaken on the systems subject to testing. For instance, in the event that there are unforeseen consequences subsequent to the pentesting operations which cause damage to the tested information system, the question of liability will have to have been addressed beforehand. The drafting of this type of document should be as accurate as possible, from possible port scanning to eventually developing malware or launching a DDOS attack.

Not only state entities are entitled to perform vulnerability assessment, private cyber red teams can also be employed. The abovementioned regulations apply to private information security companies. In the private sector, the use of penetration testing is already widespread and relies on the very notion of the consent of the rightful owner of the information systems that are to be tested. The consent, explicitly given, would mean that an operator performing a vulnerability assessment on an organisation would be fully entitled to perform his activities provided that the conditions under which they are performed are done according to strict and well-defined specifications. This is often called the 'get-out-of-jail-free card'[119] hence making the contract the cornerstone of the process. It is of a paramount importance that the cyber red teaming process is clearly bound by limitations and by a regulatory framework.[120] Companies providing such services should also be certified and proven fit to conduct such activities.[121]

The contract will have to include, for example, the following items:

- a description of the perimeter of the vulnerability assessment and its modalities (mostly technical);
- the names, roles and responsibilities of the vulnerability assessment provider;
- the need for a clear authorisation from the requester;
- specify the operations that can be conducted with and without an explicit authorisation;
- specify the material requirements that might be provided (personnel, technical etc.);
- lay out the rules for the disclosure of any information regarding the vulnerability assessment; and

[119] Kevin Mitnick and William L. Simon , The art of Intrusion, The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers, Wiley Publishing, 2005, p. 118.
[120] SANS institute papers, Guidelines for Developing Penetration Rules of Behaviour, http://www.sans.org/reading-room/whitepapers/testing/guidelines-developing-penetration-rules-behavior-259.
[121] The French ANSSI has provided a certification guideline for penetration testing service providers defining a number of criteria that these companies must meet in order to be certified. Certification requirements, February 2013, in French on the ANSSI's website, http://www.ssi.gouv.fr/IMG/pdf/RGS_PASSI_v2-0.pdf (in French).

- require that the personnel employed by the service provider have good credentials and abide by an ethics code of conduct.[122]

The legal considerations have to be integrated in the planning process and the presence of a legal advisor could be helpful to enhance the control of the activities conducted by cyber red teams, clarifying and defining the extent and scope of their activities and mapping out the potential legal risks of these activities.

Legal risks of cyber red teaming activities

The notion of the 'get-out-of-jail-free card' was mentioned earlier but it should not be used lightly as cyber red teaming, to a certain extent and when used under certain circumstances, can entail a number of consequences that present a number of risks. These risks exist whether the red teaming activities are performed by a military team or by an external service provider.

We have identified three types of immediate risk in regard to the use of cyber red teams:

- Privacy issues;
- Liability issues; and
- Copyright issues.

a. Data protection, illegal interception and possible infringements of privacy laws

Performing cyber red teaming might lead to the use of certain tools that will gather personal data in order to find vulnerabilities by the interception of data, or emails, for example. A cyber red team will gather a list of files containing personal data in order to find a way to access the targeted information system or to perform social engineering. As the vulnerability assessments will be performed on information systems that can involve public administrations or public and private companies, it is of the utmost importance that breaches of privacy regulations are avoided. These are set by, for example, Article 8 of the European Convention on Human Rights which states that 'everyone has the right to respect […] for his correspondence'.[123] The protection of correspondence entails the right to uncensored and uninterrupted communication and though the notion of 'correspondence' might be understood as referring to letters only, it is acknowledged that Article 8 also affords protection to communication via electronic means.[124]

[122] Requirement framework for the Information Security Audit Service providers (version of 14 February 2013) established by the ANSSI, http://www.ssi.gouv.fr/IMG/pdf/RGS_v-2-0_C.pdf (in French).
[123] Article 8 of the European Convention on Human Rights.
[124] See http://echr-online.com/art-8-echr/introduction#Scope of article 8 ECHR.

The processing of personal data is regulated by international treaties for NATO member states adhering to the Council of Europe Conventions and also by EU law[125] for those which are EU members. From the civil rights perspective, it is a laudable development but it can limit cyber red team activities. If the Conventions and EU law allow states to restrict the protection of privacy and personal data for national security or public safety concerns, these do not cover the case when a cyber red team is deployed in order to uncover vulnerabilities. In fact, if personal data is to be collected and used, the processor would have to undertake a declaration process to the national data protection supervisory authority in accordance with EU Directive 95/46.[126] This process must give the following information: notice, purpose, consent, security, transfer, access, accountability. Given the level of uncertainty of cyber red team activities, it might be difficult to make a declaration each time a cyber red team is to be deployed. In regard with operational concerns, it could prove counterproductive, but at the very least a consultation with the national supervisory authority could be done in order to assess the obligations which a military organisation has; in particular, certain types of data processing can be simplified or even exempted according to Article 18 of Directive 95/46.[127]

In addition to the provisions of Article 18, a personal data protection official has been appointed in the Ministries of Defence of some EU countries, including Germany. It is his task to ensure, 'in an independent manner, the internal application of the national provisions taken pursuant to this Directive'.[128] Nevertheless, the authority granting the authorisation to perform the vulnerability assessments, whether internal or external, has a duty to inform the personnel employed under its orders that their personal information might be used while these activities are being performed. The

---

[125] Convention for the Protection of Human Rights and Fundamental Freedoms as amended by Protocols No. 11 and No. 14, 4 November 1950, http://conventions.coe.int/treaty/en/Treaties/Html/005.htm.
Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, 28 January 1981, http://conventions.coe.int/Treaty/EN/Treaties/Html/108.htm.
Article 16 of the Treaty on the Functioning of the European Union (TFEU) and the common provisions provided by article 6 of the Treaty on the European Union, http://ec.europa.eu/justice/data-protection/law/treaty/index_en.htm.

[126] See section IX of the directive 95/46, *supra* note 105

[127] 'member states may provide for the simplification of or exemption from notification only in the following cases and under the following conditions:
- where, for categories of processing operations which are unlikely, taking account of the data to be processed, to affect adversely the rights and freedoms of data subjects, they specify the purposes of the processing, the data or categories of data undergoing processing, the category or categories of data subject, the recipients or categories of recipient to whom the data are to be disclosed and the length of time the data are to be stored, and/or
- where the controller, in compliance with the national law which governs him, appoints a personal data protection official, responsible in particular:
- for ensuring in an independent manner the internal application of the national provisions taken pursuant to this Directive
- for keeping the register of processing operations carried out by the controller, containing the items of information referred to in Article 21 (2),
thereby ensuring that the rights and freedoms of the data subjects are unlikely to be adversely affected by the processing operations.' Article 18,

[128] Article 18 of the directive 95/46, *supra* note 105

key issue here is to determine to what extent, in a working environment, privacy regulations may apply. The employee should not assume that what he is doing of a private nature at work will remain private, but the employer must inform its employee that his personal data might be collected during these security tests.

There is a further crucial element of this regulation, and that is the duty to notify that such collection might be occurring during vulnerability assessments. This duty to inform is a legal obligation that can be found in other branches of law such as, for instance, in the French Labour Code.[129] The person employed either in public administration, a military structure or in the private sector should not assume that his privacy is totally guaranteed as the employer has a right to monitor, to a certain extent, the activity of his employees. Naturally, the secrecy of correspondence has to be guaranteed and hence emails marked as personal should not be the object of cyber red teaming and should therefore be kept outside the scope of the team's activities. Drawing the line is difficult here and might prove impossible as the distinctions between private and public tend to be blurred. The violation of such an obligation is a criminal offence and can be prosecuted.[130] However in the case of an inadvertent disclosure of the content of an email, it is unlikely that a judge will consider it an illegal interception. To be illegal, the interception would have to have been conducted with clear intent. If the content of a private correspondence were be to become known, actions should be taken to prevent the disclosure of the data. Finally, based on paragraph 2 of Article 8 of the European Convention on Human Rights,[131] one could argue that cyber red teaming activities conducted on information systems such as military or critical infrastructure is an integral part of a national security strategy and could therefore limit the application of that provision.

In most public administrations a waiver form can be signed by government personnel in order to make them aware that, for security reasons, certain operations like cyber red teaming activities might include the collection of their data. The signing of such document could constitute clear consent for the use of personal data during cyber red team activities and indemnify the authority requesting these activities and more importantly the operators that perform such tasks. This document should be clear

---

[129] Article L2323-32 of the French Labour Code, http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006901962&cidTexte=LEGITEXT000006072050.

[130] Articles L.226-15 and L.432-9 of the French criminal code. http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006417954&cidTexte=LEGITEXT000006070719&dateTexte=20090620; http://www.legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006418513&cidTexte=LEGITEXT000006070719.

[131] '1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.'

enough and not be too general so that the validity of the consent can be acknowledged.

b. Liability issues – reparations

Cyber red teaming activities, especially non-notified ones, may have some unforeseen consequences that are outside of the defined scope and which result in collateral damage by causing disruption on third-party systems. This could happen when the use of certain tools is inappropriate and their consequences might not be known. Therefore, the question of the liability of the actors involved in these activities could, in these cases, be raised with regard to public and private persons.

In the first part of the study, we stressed that cyber red team activities could go further than pentesting, especially in the case of testing offensive capabilities. The liability of the state in conducting dangerous activities could be invoked if, for example, a cyber red team was to be using malware in order to assess certain vulnerabilities, in particular on critical infrastructure. The question of damage caused to a network owned by the authority is subject to certain questions and might imply the implementation of contingency planning measures. It could be considered that by deploying engineered malware, a state has knowingly placed its infrastructure and that of others in danger, and it seems only fair that liability is determined when damage has occurred because of neglect or wrongdoing.

In national public law, there are cases when the liability of the state can be determined and can entitle the victims to compensation and reparation for the damage. For example, a cyber red team is performing activities on the critical infrastructure of a private company. The team installs a backdoor to perform its test, but later this same backdoor is used for a real cyber attack which results in the theft of client information. Given the cost of these data breaches, and as the cyber red team can be determined to have been the origin of the fraudulent activity, the company would be entitled to ask for compensation.[132] French jurisprudence has deemed that a state's responsibility without fault could be drawn from such conduct because it engaged in what could be deemed as a hazardous activity. [133]

Another issue that can be mentioned is the question of state responsibility when cross border harm occurs, that is to say when damage is caused outside the national borders and affects a third party system. Under international law, states have a duty to monitor the cyber infrastructure under their control and prevent harmful or unlawful

[132] The cost of a data breach can be significant, In the USA, one breached file can cost up to 133 USD in processing. http://www.itworld.com/article/2833112/it-management/how-much-do-data-breaches-cost--more-than-you-think.html.

[133] Decision of the Conseil d'Etat known as 'Regnault-Desrozier', CE, 28 March 1919, after an ammunitions storage facility exploded and caused great damage in 1916. It constitutes a milestone of the recognition of the liability of state without fault on the foundation of risky activities.

cyber activities from being performed from it. If this principle of due diligence is not respected, a state would be committing an 'internationally wrongful act'.[134] For example, we can imagine the case of malware used to assess vulnerabilities that escapes the control of its creators. This scenario is very unlikely to happen but spill-over effects do exist. The case of the Stuxnet worm is a good example of malware that had behaviour which was not anticipated as it replicated throughout the world and attacked other Industrial Control Systems causing minor disruptions.[135] These events did not lead to any claims for reparations. However, if such a responsibility were to be determined; that is to say, if spreading malware were to be shown without doubt to be attributable to a particular state, then its liability could be invoked and compensation sought.[136] This risk exists, although in the case of cyber red teaming activities it remains highly unlikely.

Cyber red teaming, when performed by an external provider, also requires careful attention. It is very likely that the scope of the activities will be narrower and limited to carefully crafted boundaries. Nevertheless there are some pending issues which would derive from the obligations contained in the contract as there are many cases of risks or out of scope activities that can lead to direct consequences to the organisation such as disclosure of vulnerabilities, of damage caused to the information system.

The contract will therefore provide for the necessary limitations that a contractor will have to implement during the course of his actions, but there may be some situations where a service provider might be non-compliant in regard with the original contract that was drafted and his actions outside the scope that was originally defined. As a binding document, the provisions regarding the liability of the provider are carefully drafted to avoid damage, and more importantly to hold the contractor accountable for his actions. These obligations can include the fact for a service provider to be insured if such incidents were to occur.[137]

---

[134] Article 2 of the Articles on Responsibility of States for Internationally Wrongful Acts, 'There is an internationally wrongful act of a State when conduct consisting of an action or omission: (a) is attributable to the State under international law; and (b) constitutes a breach of an international obligation of the State'. http://legal.un.org/avl/ha/rsiwa/rsiwa.html

[135] Vincent Manzo, 'Stuxnet and the dangers of cyberwar', The National Interest, 29 January 2013, http://nationalinterest.org/commentary/stuxnet-the-dangers-cyberwar-8030

[136] 'It is a well-established rule of international law that an injured State is entitled to obtain compensation from the State which has committed an internationally wrongful act for the damage caused by it.' In the Case concerning the Gabcíkovo-Nagymaros Project, judgment of 25 September 1997, p. 81.

[137] 'All penetration testing service providers should have liability insurance sufficient to cover the costs associated with the risk of losing a client's proprietary information and any potential loss in revenue that might result from unexpected downtime caused by their activities. If the service provider does not have a liability insurance, pay attention how they specify the liability in their 'Terms and Conditions'. Management must also assure that it can recover from a loss of data during testing by having in place adequate incident response and disaster recovery plans that have been developed and verified before testing begins.' SANS paper, 'Penetration Testing: The Third Party Hacker', http://www.sans.org/reading-room/whitepapers/testing/penetration-testing-third-party-hacker-264.

c. The case of reverse engineering.

Cyber red teams may be performing reverse engineering to uncover the vulnerabilities of a computer program in order to gain access. In an attempt to mimic real-life scenarios, they might reverse-engineer in ways to improve the behaviour of malware. This is one of the techniques to better apprehend and implement efficiently an adversarial approach. These techniques are not without legal risks.

First, there is a clear risk of copyright infringements and an interesting question may arise with respect to that. In the sense of Article 4[138] of the World Intellectual Property Organisation (WIPO) Copyright Treaty (Geneva, 20 December 1996), Article 1 paragraph 3 of the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs, and corresponding national laws, a malware is a 'computer program' and reverse engineering by a cyber red team is not covered by the exceptions provided by law.[139] However there is a need to weigh the proportionality between the requirement to use the malware to improve the security of a government CIS, and the somewhat 'atrophied' rights of the author of the malware who let it out into the wild. Once it is out, does the creator of a malware still have any rights over it?[140] Criminality remains a criterion and it is difficult to build an exception to the copyright compliance obligation as the criminal intent might not be obvious when engineering the malware. In fact, from the copyrights law point of view, it is merely the expression of an idea. Nevertheless, the argument of public interest can be a powerful one in regard with cyber red teaming activities.

To conclude, the copyright issue should be carefully mapped out before engaging in these activities for a military cyber red team or simply excluded from the scope of the activities envisioned if they are to be performed by a private entity.

[138] Article 4 'Computer programs are protected as literary works within the meaning of Article 2 of the Berne Convention. Such protection applies to computer programs, whatever may be the mode or form of their expression'.
[139] For example, Article 6 of the Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 that states as an exception the decompilation of software in order to achieve interoperability.
[140] See 'Copyright Protection for Virus Authors, Establishing Protection for Authors Irrespective of the Merits of Their Creation', https://www.duo.uio.no/bitstream/handle/10852/22917/JeremyxLundex-xUiO-Thesis.pdf?sequence=1.

Conclusion

Cyber red teams focus on threats from adversaries in the cyber world. They mimic the mind-set of attackers, regardless of their motivations, in order to improve the security of one's own organisation. In the military realm, the need to understand the adversary is the cornerstone of any sound strategy and their implementation is a legitimate endeavour that needs to be considered, especially when testing procedures and methodologies.

In this study, organisational, legal and technical considerations of the cyber red teaming concept were discussed and presented. The requirements and challenges were presented in order to assess the feasibility and the conditions under which the development of such a capability can be possible. More importantly, this can be determined according to the level of ambition and the resources available.

The need for a framework is of the utmost importance in order to formalise a process. Although there are serious considerations and risks associated with the use of cyber red teams, the discussion on whether to develop cyber red teams is a relevant one and this is good practice in order to implement a sound cyber security policy. This decision is dependent on cyber threat perception, technical capabilities, the opinions of legal experts, organisational limitations and advantages, and ultimately on the high-level decision-makers.