Military Activities and Cyber Effects (MACE) Taxonomy

Melanie Bernier
DRDC CORA

DRDC CORA TM 2013-226
December 2013

Defence R&D Canada
Centre for Operational Research and Analysis

Information Management Operational Research Team

Military Activities and Cyber Effects (MACE) Taxonomy

Melanie Bernier
DRDC CORA

Defence R&D Canada – CORA

Technical Memorandum
DRDC CORA TM 2013-226
December 2013

Principal Author

Melanie Bernier

Information Management OR Team

Approved by

Robert Burton

Section Head Joint Systems Analysis

Approved for release by

Paul Comeau

DRDC CORA Chief Scientist

This research is sponsored by the Chief of Force Development Director General Cyber through the Director Cyber Force Development as part of DRDC ARP 15bh project on Modeling and Simulation of Cyber Effects and Capabilities on Command and Control. The information and opinions expressed herein remain those of the author and do not represent, or otherwise reflect, any official opinion of the Department of National Defence, the Canadian Armed Forces, or the Government of Canada.

Defence R&D Canada – Centre for Operational Research and Analysis (CORA)

Abstract

Malicious cyber activities are continually growing both in number and in complexity. There are many types of cyber attacks that exist and each can produce a range of effects. In order to facilitate an improved shared understanding of threats in the cyber environment among military operators, we propose in this report a taxonomy for Military Activities and Cyber Effects (MACE). The MACE taxonomy was originally developed as the foundation for the modeling, simulation and experimentation of cyber attacks and the effects they can produce, but was then expanded to describe the linkages to military activities and their desired effects. It consists of the following six categories: Attack Types, Levels of Access, Attack Vectors, Adversary Types, Cyber Effects, and Military Activities. Together these can provide the underlying structure for the development of a threat model or can easily provide the details required to develop scenario vignettes for cyber related experiments and exercises. This report describes in detail the six categories of the taxonomy.

Résumé

Le nombre et la complexité des cyberattaques augmentent sans cesse. Or, il existe plusieurs types de cyberattaques, donc chacune peut entraîner plusieurs conséquences. Afin de favoriser une meilleure compréhension commune des cybermenaces dans les milieux militaires, le présent rapport propose une taxonomie des activités militaires et des conséquences informatiques (AMCI). Originellement développée pour modéliser et simuler les cyberattaques et leurs conséquences ainsi que faire des expériences à ce propos, la taxonomie AMCI a ensuite été amplifiée afin de décrire les liens avec les activités militaires et les effets voulus de celles-ci. Elle compte six grandes catégories : types d’attaques, degrés d’accès, vecteurs d’attaque, types d’adversaires, conséquences informatiques et activités militaires. Dans leur ensemble, ces catégories peuvent former la structure sous-jacente au développement d’un modèle de menaces, et elles peuvent donner rapidement les détails nécessaires au développement de scénarios destinés à des expériences et exercices touchant les cybermenaces. Le rapport décrit en détail les six catégories de cette taxonomie.

This page intentionally left blank.

Executive summary

Military Activities and Cyber Effects (MACE) Taxonomy:

Melanie Bernier; DRDC CORA TM 2013-226; Defence R&D Canada – CORA; December 2013.

Introduction: Government departments and military forces have become increasingly reliant on computer network technologies to conduct their day to day tasks and operations. Every year, we detect more attacks than the year before and those seeking to infiltrate, exploit or attack our cyber systems are getting more sophisticated and better resourced. It is becoming ever more apparent that cyber attacks have the potential to be extremely disruptive to any cyber dependent organization. There is a large variety of cyber attack types and each can produce a range of effects. In order to facilitate an improved shared understanding of threats in the cyber environment among military operators, the Defence Research and Development Canada (DRDC) Centre for Operational Research and Analysis (CORA) established a research project to investigate the impact of cyber effects on command decisions and how to integrate cyber capabilities into the operational planning process. As part of this research and in collaboration with the Royal Military College of Canada's (RMCC) Computer Security Laboratory, DRDC CORA developed the framework for a Military Activity and Cyber Effects (MACE) taxonomy which classifies cyber attacks based on the level of access required to launch the attack, the effects they can produce and the military activities they can be used for.

Results: The MACE taxonomy was originally developed to provide the foundation for the modeling, simulation and experimentation of cyber effects and threats in a military setting. It consists of six main categories which are described as follows.

- Attack Types: This category covers the most significant types of cyber attacks. This report does not attempt to provide a complete comprehensive list as new malicious computer programs (malware) are created on a daily basis but instead concentrates on the more broad-based cyber attacks that have been observed in large computer networks.
- Levels of Access: This category describes the different levels of access to the targeted system or network that attackers may require in order achieve a type of attack. The level of access determines the restrictions on and privileges of what an attacker can do.
- Attack Vectors: This category includes the methods and tools used to infiltrate computers and install malicious software. The delivery methods require some level of effort from the attacker in order to launch the attack while the delivery tools often do not require as much of an effort as they can spread and infect other computers autonomously.
- Adversary Types: This category identifies the various types of cyber attackers. The types are differentiated using a combination of skill level, maliciousness, motivation, and method used.

- Cyber Effects: This category describes the effects that can be produced in the cyber environment by employing the various cyber attacks. Each effect can affect the targeted systems themselves or the information that resides within them.
- Military Activities: This category includes the military effects that can be produced in the cyber environment. It denotes the military context and language in this taxonomy that enables a common understanding between defence departments and other government departments.

The taxonomy was developed in three phases; each phase is described in detail in this report. The first phase classified the various types of cyber attacks and includes the first four categories of the taxonomy: Attack Types; Levels of Access; Attack Vectors; and Adversary Types. The second phase characterised the cyber effects and describes the various effects that could be achieved in the cyber environment as well as which of the cyber attacks can lead to those effects. The third and final phase brought in the military context and describes the desired effects from the military perspective and how these relate to the cyber effects and subsequently the cyber attacks.

Significance: The MACE taxonomy was originally developed to gain a better understanding of the effects achieved by the various cyber attacks. The main purpose was to then simulate these effects in support of training and experimentation. Through these methods, we may begin to understand the effects that cyber attacks may have on military commanders' decision-making capabilities and thus on mission effectiveness. In fact, Phase 2 of the taxonomy was used as the foundation for the development of a series of cyber events/vignettes that was used in recent Canadian Armed Forces (CAF) experiments and exercises. A total of sixteen scenario events were developed to evenly span the range of cyber effects and attacks presented in this report and in turn provided sufficient variety and realism to present the experiment participants with a cross-section of potential cyber events to address.

The taxonomy can also be applied as a potential component of a cyber threat model. The concise description of the mechanisms of cyber attacks is a key element in planning and executing defences against such attacks. Describing an adversary's objective in terms of the six categories of the MACE taxonomy could be the first step towards describing a cyber threat. Overlaying such a threat description with a framework like the MITRE Corporation's Cyber Preparedness methodology or Sandia National Laboratories' Operational Threat Assessment methodology could potentially provide an effective threat model.

Future plans: The development of a cyber threat framework and model along with the potential application of the MACE taxonomy will be investigated further in future work within the Security and Defence Metrics work stream of the Cyber Decision Making and Response project within the DRDC Cyber Science and Technology Program

Sommaire

Military Activities and Cyber Effects (MACE) Taxonomy:

Melanie Bernier ; DRDC CORA TM 2013-226 ; R & D pour la défense Canada – CARO; décembre 2013.

Introduction : Pour mener à bien leurs activités et opérations quotidiennes, les organismes gouvernementaux et les forces militaires dépendent de plus en plus des réseaux informatiques. Or, d'année en année, nous voyons de plus en plus d'attaques contre ces réseaux, et ceux qui cherchent à infiltrer, attaquer ou exploiter nos systèmes informatiques disposent d'un nombre grandissant de ressources et sont de plus en plus sophistiqués. Il est de plus en plus évident que les attaques informatiques peuvent être extrêmement dommageables à tout organisme qui dépend de ses ressources informatiques. Il existe plusieurs types de cyberattaques, donc chacune peut entraîner plusieurs conséquences. Afin de favoriser une meilleure compréhension commune des cybermenaces dans les milieux militaires, le Centre d'analyse et de recherche opérationnelle (CARO), de Recherche et développement pour la défense Canada (RDDC) a lancé un projet de recherche visant à étudier l'effet des conséquences informatiques sur les décisions du commandement, et comment intégrer les capacités informatiques au processus de planification opérationnelle. Dans le cadre de ces recherches, et en collaboration avec le laboratoire en sécurité informatique du Collège militaire royal du Canada (CRMC), le CARO de RDDC a élaboré le cadre d'une taxonomie des activités militaires et des conséquences informatiques (AMCI), en fonction du niveau d'accès nécessaire pour lancer les attaques, les conséquences de ces attaques et les activités militaires pour lesquelles elles peuvent être utiles.

Résultats : La taxonomie AMCI a été originellement développée pour modéliser et simuler les cyberattaques et leurs conséquences ainsi que faire des expériences à ce propos dans un contexte militaire. Elle compte six grandes catégories dont voici la description.

- Types d'attaque : types de cyberattaques les plus importants. Le rapport ne cherche pas à dresser une liste exhaustive des attaques, car on crée tous les jours de nouveaux maliciels (programmes malveillants); elle est plutôt axée sur les cyberattaques de plus grande envergure observées contre les réseaux importants.
- Degrés d'accès : les niveaux d'accès à un système ou un réseau dont un attaquant a besoin pour mener un type d'attaque précis. C'est le degré d'accès qui détermine les restrictions et les droits d'accès, c'est-à-dire ce qu'un attaquant peut faire.
- Vecteurs d'attaque : méthodes et outils utilisés pour infiltrer un système et y installer des maliciels. Les méthodes d'infiltration exigent de la part de l'attaquant un certain degré d'efforts pour lancer l'attaque; les outils d'infiltration réduisent souvent cet effort, car ils peuvent se propager et infecter d'autres systèmes de façon autonome.
- Types d'adversaires : divers types d'attaquants. On distingue ces types selon le degré d'habileté, la malice, les motivations et les méthodes utilisées.
- Conséquences informatiques : effets dans l'environnement informatique visé des diverses cyberattaques. Chaque effet peut toucher les systèmes eux-mêmes ou les données qu'ils renferment.

- Activités militaires : conséquences sur le plan militaire des attaques dans l'environnement informatique. C'est la catégorie de cette taxonomie qui, à l'aide du contexte et du vocabulaire militaires, favorise une compréhension commune entre les organismes de défense et les autres ministères.

Cette taxonomie a été développée en trois phases, et le rapport décrit chacune en détail. Dans la première phase, nous avons classé les divers types de cyberattaques et ainsi créé et détaillé les quatre premières catégories de la taxonomie : types d'attaques, degrés d'accès, vecteurs d'attaque et types d'adversaires. Dans la deuxième phase, nous avons caractérisé les conséquences informatiques, décrit les divers effets qu'on peut atteindre dans l'environnement informatique et cerné les types d'attaque pouvant mener à ces effets. Dans la troisième et dernière phase, nous avons intégré à cette taxonomie le contexte militaire afin de décrire les effets voulus d'un point de vue militaire et comment ces effets sont liés aux conséquences informatiques et donc aux attaques ayant mené à ces conséquences.

Portée : La taxonomie AMCI a été originellement développée pour mieux comprendre les effets entraînés par les divers types de cyberattaques, afin de simuler ensuite ces effets aux fins d'instruction et d'expérimentation. Nous avons pu ainsi mieux comprendre les conséquences de ces cyberattaques sur les capacités du commandement de prendre des décisions et, par ricochet, sur l'efficacité des missions. En fait, la phase 2 de l'élaboration de la taxonomie a aussi servi à élaborer des événements ou vignettes utilisés dans des expériences et exercices récents des Forces armées canadiennes. En tout, seize événements ont été créés pour les scénarios afin d'illustrer toute la gamme des cyberattaques et de leurs effets, tels que présentés dans le rapport, et ce qui a représenté une variété et un réalisme suffisant pour soumettre aux participants une bonne variété de cyberattaques à contrer.

On peut aussi intégrer cette taxonomie à un modèle des cybermenaces. Décrire succinctement les mécanismes des cyberattaques est essentiel afin de pouvoir prévoir puis appliquer les mesures de défense contre ces attaques. Aussi, pouvoir décrire l'objectif d'un attaquant à l'aide des six catégories de la taxonomie AMCI peut être le premier élément de description d'une cyberattaque. Doublée d'un cadre comme la méthodologie de préparation informatique (Cyber Preparedness methodology) de MITRE Corporation ou la méthodologie d'évaluation des menaces opérationnelles (Operational Threat Assessment) de Sandia National Laboratories, une telle description des menaces peut constituer un modèle de menaces réellement utile.

Perspectives : Nous prévoyons développer un cadre et un modèle des cybermenaces, et possiblement y appliquer la taxonomie AMCI dans nos travaux effectués pour les indices de mesure en matière de cybersécurité et de cyberdéfense, dans le cadre du projet Prise de décision et réaction dans le cyberespace du Programme de cybertechnologie et cyberscience de RDDC.

Table of contents

List of figures

List of tables

Acknowledgements

The author would like to thank the following people:

Prof. Sylvain (Sly) Leblanc and his team at the Royal Military College of Canada for conducting the initial research for the taxonomy.

Maj Erik Couture, Capt Desmond Gosse, MCpl Daniel Rosati, Bob Miller and Joanne Treurniet for taking the time and reviewing the first draft of this report. Ian Chapman for agreeing to perform the peer review of the final version of this report. All of your comments and suggestions were greatly appreciated.

I would especially like to again thank Prof. Leblanc, Capt Gosse, and Joanne Treurniet for their constant support and advice throughout the development of the taxonomy and of this report.

This page intentionally left blank.

1 Introduction

Malicious cyber activities are growing both in number and in complexity. Every year, we detect more attacks than the year before and those seeking to infiltrate, exploit or attack our cyber systems are becoming more sophisticated and better resourced [1]. Consider that a decade ago, viruses were used by organizations or individuals for mostly criminal activities, such as credit card fraud and other methods of financial gain. As recently as five years ago cyber attacks evolved to be more used for political protest in times of war/conflict such as the 2007 cyber attack on Estonia [2] and the 2008 cyber attack on Georgia [3]. Today, we are increasingly faced with more sophisticated cyber attacks like GhostNet [4], designed for cyber espionage or Stuxnet [5], intended for sabotage.

Government departments and military forces have become increasingly reliant on computer network technologies to conduct their day to day tasks and operations. It is becoming ever more apparent that cyber attacks have the potential to be extremely disruptive to any network dependent organization. This was recognized in the 2008 Canada First Defence Strategy [6] where the need was stated for “a modern, well-trained and well-equipped military with the core capabilities and flexibility required to successfully address both conventional and asymmetric threat, including terrorism, insurgencies and cyber attacks”. This need has been reinforced by the recent cyber attacks on three Government of Canada departments, where the Treasury Board, the Department of Finance, and Defence Research and Development Canada (DRDC) were victims of cyber espionage attempts [7].

There is a large variety of cyber attack types and each can produce a range of effects. In order to facilitate an improved shared understanding of threats in the cyber environment among military operators, the DRDC Centre for Operational Research and Analysis (CORA) established a research project to investigate the impact of cyber effects on command decisions and how to integrate cyber capabilities into the operational planning process [8]. As part of this research and in collaboration with the Royal Military College of Canada’s (RMCC) Computer Security Laboratory, DRDC CORA developed the framework for a Military Activity and Cyber Effects (MACE) taxonomy which classifies cyber attacks based on the level of access required to launch the attack, the effects they can produce and the military activities they can be used for. Portions of this taxonomy have been applied to create cyber events and scenario injects that simulate the cyber effects desired for use in military experiments and exercises.

1.1 What is a Taxonomy?

The Department of National Defence (DND) Defence Terminology Bank [9] defines taxonomy as “a classification system that provides the basis for classifying objects for identification, retrieval and research purposes.” In The Truth about Taxonomies [10], Bruno and Richmond define taxonomy as “the science of classification according to a pre-determined system, with the resulting catalog used to provide a conceptual framework for discussion, analysis, or information retrieval. In theory, the development of a good taxonomy takes into account the importance of separating elements of a group (taxon) into subgroups (taxa) that are mutually exclusive, unambiguous, and taken together, include all possibilities. In practice, a good taxonomy should be simple, easy to remember, and easy to use.” Based on this and as described in another taxonomy paper more specific to cyber security/defence from Sandia National Laboratories [11], a good taxonomy will exhibit the following characteristics:

- Mutually exclusive: classifying in one category excludes all others because categories do not overlap;
- Exhaustive: taken together, the categories include all possibilities;
- Unambiguous: clear and precise so that classification is not uncertain, regardless of who is classifying;
- Repeatable: repeated applications result in the same classification, regardless of who is classifying;
- Accepted: logical and intuitive so that categories could become generally approved; and
- Useful: could be used to gain insight into the field of inquiry.

These characteristics are a suitable guideline for assessing a taxonomy but it should be noted that taxonomies are only an approximation of the reality [9] and that there is no perfect taxonomy. A satisfactory taxonomy may be found to be lacking on some of these attributes.

1.2 Purpose and Scope

The purpose of this report is to propose a taxonomy for military activities and cyber effects that will provide a common framework for military cyber operators and defenders to assist in the understanding of the threats they face. The taxonomy was originally developed as the foundation for the modeling, simulation and experimentation of cyber attacks and the effects they can produce but was then expanded to describe the linkages to military activities and their desired effects. As a descriptive taxonomy, it will allow military audiences, who may not have extensive experience dealing with cyber attacks, to communicate more effectively within their environment as well as with other government departments and allow them to understand the potential effects and scope of these attacks using a common language.

1.3 Report Structure

This report is organized as follows:

- Section 1 provides background, scope, and purpose;
- Section 2 provides an overview of the MACE taxonomy;
- Section 3 describes the elements developed in the first phase of the taxonomy consisting of the classification of the cyber attacks;
- Section 4 describes the second phase by characterizing the effects that can be produced by the cyber attacks;
- Section 5 describes the third and final phase and provides the representation of the desired effects from the military perspective;

- Section 6 discusses the application of the MACE taxonomy and potential areas of future work; and
- Section 7 concludes the report.

2 MACE Taxonomy Overview

To help inform the motive for developing the MACE taxonomy, a review of existing taxonomies related to the characterisation of cyber attacks and effects is presented in Section 2.1, while Section 2.2 outlines the overall view of the MACE taxonomy.

2.1 Survey of Existing Relevant Taxonomies

An initial survey of previous work in this field was conducted by RMCC prior to developing the first phase of the MACE taxonomy in 2010 and focused mostly on the characterization of cyber attacks. In this section, the initial review by RMCC [12] is presented and updated. It is also extended with additional work focussed on characterizing the effects of the attacks.

There are many previous works on taxonomies related to cyber attacks, threats and vulnerabilities. Some include the development of taxonomies for specific attack types, such as computer worms [13], or Denial of Service attacks [14]. These taxonomies tend to be very detailed, but narrow in focus. Other taxonomical work has focused on specific network environments, such as the 3G cell network. The taxonomy of Kotapati et al. [15] is based on the access level (physical and system) to 3G network infrastructure required by the attacker to launch an attack. Although this approach is limited to the 3G environment, it was found to have merit by RMCC and was considered in the development of the "Levels of Access" category of the MACE taxonomy. Other taxonomies of computer and network attacks have been created to classify specific attacks. The taxonomy proposed by Hansman and Hunt [16] is multi-dimensional, with categories for attack vectors, targets, vulnerabilities and payloads. This work allows for detailed characterization of a broad spectrum of attacks, but the purpose is to describe actual known and new attacks, such as Code Red, Slammer, and Melissa and consequently it was not suited for the MACE taxonomy.

Another approach found in literature on cyber attack taxonomies is to classify the type of attackers, their skill level and motivation. Meyers et al. [17] present a good overview of previous work in characterizing the cyber adversary and proposed a taxonomy of the different types of adversaries and their corresponding methods, motivations, maliciousness, and skill levels. This work was found to be thorough and was used as the basis for the adversary category within the MACE taxonomy.

The taxonomies reviewed in more recent papers not only describe the types of attacks but also consider the impacts of the attacks and the possible defences. AVOIDIT [18] was created by a group of researchers from the University of Memphis in support of the US Navy's Office of Naval Research. It describes attacks using five classifications: attack vector, operational impact, defence, informational impact and target. Along a similar approach, Applegate and Stavrou's taxonomy [19] classifies cyber events and exposes logical connections and links between different actors, types of attacks and vectors used, and various types of impact associated with each event. The taxonomy is divided into categories and subjects where categories are the classifications that are applied to subjects and where subjects represent the real world events classified as cyber conflict. The categories component has some similarities to the AVOIDIT taxonomy.

Although these last two taxonomies take into consideration the operational, informational and systems impact which can be related to military operations, they do not consider the desired effects of cyber attacks in a military context. For this reason, the MACE taxonomy was developed, which not only describes cyber attacks but also describes the effects of the attacks and links these to military effects.

2.2 An Overview of the MACE Taxonomy

The MACE taxonomy was originally developed to provide the foundation for the modeling, simulation and experimentation of cyber effects and threats in a military setting. The taxonomy classifies cyber attacks based on the level of access required to launch the attack, the cyber effects the attack can produce and the military activities it can be used for. It consists of six main categories which together can provide the underlying structure for the development of a threat model or it can easily provide the details required to develop scenario vignettes for cyber related experiments and exercises. The six categories are denoted in Figure 1 and consist of the following.

- Attack Types: This category covers the most significant types of cyber attacks. This report does not attempt to provide a complete comprehensive list as new malicious computer programs (malware) are created on a daily basis, but instead concentrates more broadly on the cyber attacks that have been observed in large computer networks.
- Levels of Access: This category describes the different levels of access to the targeted system or network that attackers may require in order to launch a type of attack. The level of access determines the restrictions on and privileges of what an attacker can do at the various levels.
- Attack Vectors: This category includes the methods and tools used to infiltrate computers and install malicious software. The delivery methods require some level of effort from the attacker in order to launch the attack while the delivery tools often do not require as much of an effort as they can spread and infect other computers autonomously.
- Adversary Types: This category identifies the various types of cyber attackers. The types are differentiated using a combination of skill level, maliciousness, motivation, and method used.
- Cyber Effects: This category describes the effects that can be produced in the cyber environment by employing the various cyber attacks. Each effect can affect the targeted systems themselves or the information that resides within them.
- Military Activities: This category includes the military effects that can be produced in the cyber environment. It denotes the military context and language to this taxonomy that enables a common understanding between defence departments and other government departments.

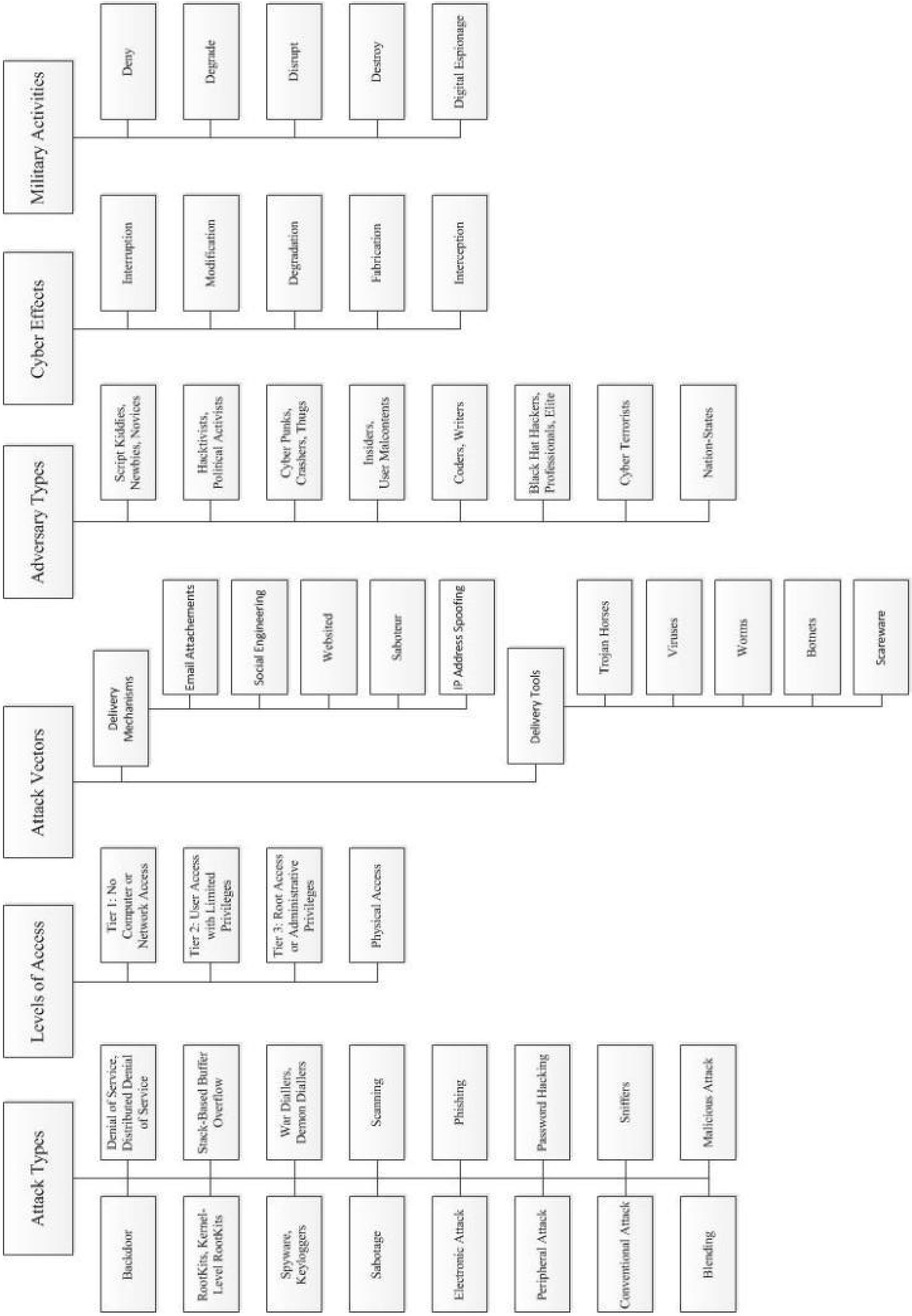

Figure 1: MACE Taxonomy Overview Diagram

The taxonomy was developed in three phases. The first phase, as described in Section 3, classified the various types of cyber attacks. It included the first four categories of the taxonomy: Attack Types; Levels of Access; Attack Vectors; and Adversary Types. The second phase (see Section 4) characterised the cyber effects, which is the fifth category of the taxonomy. It describes the effects that could be achieved in the cyber environment as well as which of the cyber attacks can lead to those effects. The third and final phase brought in the military context (see Section 5). It represents the military activities within the cyber environment and describes the desired effects from the military perspective and how these relate to the cyber effects and subsequently the cyber attacks. Overall, as discussed in Section 6, describing an adversary's objective in terms of these six categories would provide the first step required in describing a cyber threat. Overlaying such a threat description with a framework like the MITRE Corporation's Cyber Prep methodology [20] or Sandia National Laboratories' Operational Threat Assessment methodology [21] could potentially provide a full cyber threat description.

3 Phase 1: Cyber Attack Classification

The first phase of the taxonomy was conducted by the Computer Security Laboratory at the RMCC for DRDC CORA [22][23]. It involved the classification of cyber attacks based on the level of access that the attacker required to launch the attack. The initial research conducted provided four of the six categories of the MACE taxonomy: Attack Types; Levels of Access; Attack Vectors; and Adversary Types. Section 3.1 describes the levels of access and the classification of the various types of cyber attack by their required minimum level of access. Section 3.2 describes the methods and tools used to deliver malicious software while Section 3.3 describes the different types of adversaries.

The techniques described in the sub-sections below can involve any of the stages of a cyber attack, also known as the cyber attack kill chain [24][25]. Most adversaries will follow a common series of seven steps in order to execute an attack, as shown in Figure 2.

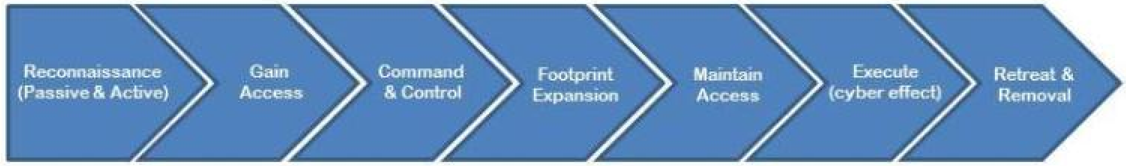

Figure 2: Stages of a Cyber Attack (modified from [24])

For the purpose of this paper the seven stages of a cyber attack are described as follows:

- Reconnaissance. This is considered the planning step of an attack where the adversary gathers as much information as possible about the target prior to the attack. Passive reconnaissance involves techniques such as gathering publicly available information, using search engines, and dumpster diving (i.e. going through the bins). Active reconnaissance on the other hand involves using tools to actively interact with the target, such as network scanning [26].
- Gain Access. This step is the initial intrusion into the target network. Through the reconnaissance step the adversary will have identified and correlated vulnerabilities that can be exploited to penetrate the network and gain initial access. This step can also be achieved through user exploitation such phishing or social engineering techniques [24].
- Command and Control. Typically, in malware attacks the compromised system must call out to a control server to send out found information or to receive additional instruction. The malware will establish a command and control channel with the control server (often through encrypted channels that are hard to detect) and in turn provide the adversary with the means to get inside the target network [24][25].
- Footprint Expansion. In the case of data exploitation or if the goal is simply to infect as many systems as possible, the malware will need to move laterally within the network from system to system to either find the target data or to infect each of the systems found [24]. Another facet of this stage is privilege escalation where the adversary can

escalate from limited privileges (user access) to administrator privileges (root access) so that they are not constrained to any specific part of the network.

- Maintain Access. This stage involves maintaining long-term access to the target system and network, which allows the adversary the benefits of time to collect the information they need for the purpose of their attack. Access can be maintained by launching virtual network clients from within the network to provide access to external systems, and similar services like File Transfer Protocol (FTP) and Secure Shell (SSH), or by uploading rootkits, backdoors and Trojans (as described in sections 3.1.3 and 3.2.2).
- Execute Attack. The adversary takes actions that accomplish his objectives. The actions taken will depend on the goal of the adversary where the most common may be exfiltration of data but could also involve the modification, fabrication, interception and even destruction of data (see section 4.2).
- Retreat and Removal. This phase closes the loop, where the adversary removes all evidence of his presence on the target system and network. It should be noted that a skilled adversary will always cover their tracks to avoid early detection. Gaining root level access and administrative access is a big part of hiding their presence as they can remove log entries, deactivate alarms, and even upgrade or patch outdated software in which a vulnerability was exploited.

3.1 Cyber Attacks by Level of Access Required

In the RMCC report [23], there are four levels of access identified (as depicted in Figure 3). The four levels are described as follows:

- Tier 1: No Privilege Required. These attacks require no access to the target computer. They consist of attacks that gather information on the target and attacks that attempt to gain access to or deny resources to a target computer.
- Tier 2: User Access with Limited Privileges. These attacks require a minimum of *user* access to the target computer. This can be done either remotely by hacking into a computer, from across the internet or over a network, or it can be done physically by gaining physical access to a computer.
- Tier 3: Root Access or Administrative Privileges. After gaining *root* access, also known as *administrative* privileges in the case of Windows operating systems, the attacker has complete freedom of action on the computer, with the ability to execute arbitrary code.
- Physical Access. This refers to the physical offensive capabilities in the range of network infrastructure, either overt or covert. It is therefore a product of adversary capabilities versus physical defences, denoting the adversary's ability to exert physical influence upon elements of a computer network system.

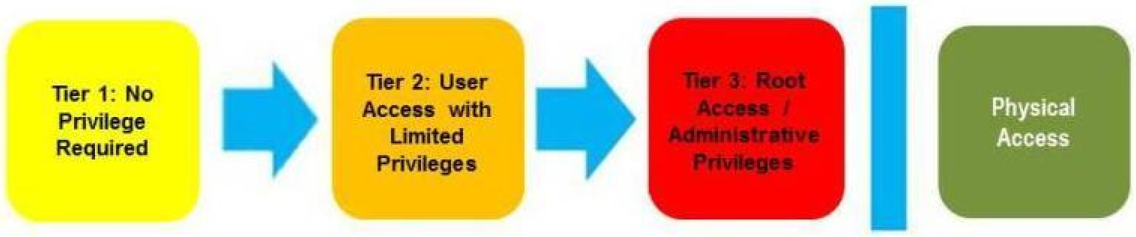
Tier 1: No Privilege Required
Tier 2: User Access with Limited Privileges
Tier 3: Root Access / Administrative Privileges
Physical Access

Figure 3: Levels of Computer / Network Access

There exists an implied hierarchy in the levels of access, where the access level used to classify the attack represents the minimum access required in order to carry out the intended attack. Therefore any attack type requiring Tier 1 access can also be prosecuted with Tier2 and Tier 3 access. Note that access can also be progressively escalated to Tier 3. For example, attacks carried out with Tier 1 access can be used to obtain user information that would enable an escalation to a Tier 2 access followed by a Tier 3 access. There is no implied hierarchy between Physical Access and Tiers 1, 2 and 3; although Tiers 1, 2 and 3 may be achieved through Physical Access.

There is a wide variety of attacks in operations world-wide and it is not possible to provide a complete comprehensive list as new malicious computer programs (malware) are created on a daily basis. In the sub-sections below, the most significant types of attacks are described and classified using the minimum level of access required to execute them. Note that these types of attacks are described in greater detail in the RMCC report [23].

3.1.1 Attacks Classified under Tier 1 Access

As described earlier, Tier 1 attacks can be implemented with absolutely no access to the target computer. They consist of attacks that gather information on the target and attacks that attempt to gain access to or deny resources to a target computer.

- Denial-of-Service Attack (DoS)/Distributed DoS (DDoS): An activity that can be launched directly across the internet, where the attacker only needs to know the target computer's internet protocol (IP) address to commence the attack. There are several forms of DoS/DDoS attacks but all consist of an attacking computer or multiple computers sending requests, packets or bad communications to a target computer. The difference between a DoS and a DDoS is that a DDoS attacks on a far greater scale, employing potentially thousands of computers to aid in the attack.
- Stack-based Buffer Overflow: An activity that exploits vulnerabilities in computer programs to sneak additional code into the target computer's operating system stack. This can be done remotely over a network or in Tier 2 depending on whether the computer program abused can be run remotely, such as over a network or on a website. It can also be run directly on the targeted computer itself. Stack-based buffer overflow attacks can allow the attacker to run any command he wants, referred to as arbitrary code, as long as the program targeted has the privileges to perform this action.
- War Diallers, Demon Diallers, and War Drivers: Software that is used to gain access to a computer network from the outside. The software tries to penetrate a target's network

through a vulnerable modem or in the case of War Drivers, a wireless network. Once a network is accessed the attacker will have the same access privileges as the user of the remote control software on the target computer. This means that the attacker can then proceed to Tier 2 or 3 attacks depending on the access gained.

- Scanning: Consists of a variety of activities that are used to try to discover the network configuration of a target. This can better prepare attackers for carrying out future attacks on the network. Furthermore, vulnerability scanners can allow the attacker to discover whether a target has any common security holes open to abuse in a future attack.
- Phishing: A type of social engineering attack that consists of either mass emailing of email addresses hoping that at least a few recipients will be tricked by the email, or emailing a specific email address with more thought and care (referred to as spear phishing). The emails try to convince the recipient to take an action, such as downloading an attachment containing malware, or convince the recipient to follow a link to a website that has scripts that will download malware to the target computer. Other possible goals other than infiltrating computers with malware are to convince users to give up their personal information, credit card details, or their usernames and passwords. In general, Phishing attacks are broadcast to a large audience rather than being targeted. Spear Phishing is a variant that targets specific individuals with detailed and often personal details. Whaling is another variant that is extremely sophisticated as these attacks are specifically designed to gain access to the systems of highly placed individuals.

3.1.2 Attacks Classified under Tier 2 Access

Tier 2 attacks require a minimum of user access to the target computer. This can be done either remotely by hacking into a computer, from across the internet or over a network, or it can be done by gaining physical access to a computer. Although there are limited privileges at this access level, there are a number of attacks available to the attacker.

- Password Hacking/Cracking: The process of discovering usernames and passwords on a computer or a network from data that has been stored in or transmitted by a computer system. This allows the attacker to be able to log in to any person's computer on a network or access administrator accounts, giving access to Tier 3. Most methods of cracking passwords involve using a computer program to automate the process.
- Sniffers: Computer programs that read data passing across a computer network in real time. This includes passwords and usernames transmitted over the network and can also reveal Domain Name System (DNS) queries and responses as well as email messages sent by other users. Overall, a sniffer can eavesdrop on anything not encrypted that is passed over the computer's attached local area network (LAN). It can also aid in hijacking sessions between two computers and allow the attacker to execute arbitrary code on the hijacked computer.
- Other Malicious Attacks: (also known as malware) Software or program code designed to disrupt or deny operations, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources and other abusive behaviour.

Some malware require Tier 3 access to be executed while others can be run with only Tier 2 access.

3.1.3 Attacks Classified under Tier 3 Access

Tier 3 attacks require root access or administrative privileges (in the case of Windows operating systems). At this stage, the attacker has complete freedom of action on the computer, with the ability to execute arbitrary code.

- Backdoors: Software that allows an attacker to re-enter the target computer without having to use the same entry point as before. This allows an attacker to bypass the authentication mechanisms on an infiltrated computer and grants the attacker all the abilities of control over the computer that they would have if they had logged in legitimately to the computer. Therefore if a defender changes his password, the attacker would still have access.
- RootKit/Kernel-level RootKit: Software that acquires and maintains privileged access to the operating system while hiding its presence by challenging normal operating system behavior. A rootkit has three goals: to run without restriction on a target computer; to elude being detected by the computer or an installed security product; and to conduct its attack, such as stealing passwords or network bandwidth, or installing other malicious software. There are two fundamental types of rootkits, user-mode rootkits and kernel-mode rootkits. The difference is based on the levels at which they operate and the type of software they change or replace [27].
- Spyware/Keyloggers: Software that can be installed on a target computer that collects small pieces of information about users without their knowledge. This software can be installed once the defences of a computer are breached such as when an attacker discovers login credentials, or by such means as computer worms or Trojan horses (see Section 3.2), or by being automatically downloaded when a user visits a website that exploits security holes in their web browser. Privacy invasion software is normally hidden from the user and difficult to detect.
- Malicious Attacks with Full Privileges: As in Section 3.1.2, but where the attacker has full privileges.

3.1.4 Attacks Classified under Physical Access

Physical access refers to the physical offensive capabilities in the range of network infrastructure, either overt or covert. It is a product of adversary capabilities versus physical defences, denoting the adversary’s ability to exert physical influence upon elements of a computer network system.

- Sabotage: The covert application of physical effects in order to compromise, deny, degrade, disrupt, or destroy elements of a computer network system. An adversary employing sabotage gains proximity through subterfuge rather than manoeuvre or force of arms. Actions of the saboteur may include, but are not limited to, explosive demolition, cable cutting, physical reconfiguration of network components, damage to wireless transmission equipment, and assassination, bribery or coercion of critical network personnel.

- Electronic Attack: The use of electromagnetic (EM) radiation against physical network components to disrupt or deny computer network service, or to physically destroy computer network hardware or data residing therein. Jamming involves the transmission of radio signals to deliberately interfere with communications on targeted frequencies by overwhelming them with radio 'noise'. Jamming may prevent wireless network traffic.
- Peripheral Attack: Computer systems are designed to make use of a wide range of peripheral devices and services such as those that use the Universal Service Bus (USB) or wireless connections (Wi-Fi); physical access to these services can be sufficient to compromise a computer system.
- Conventional Attack: The overt application of violent physical forces to computer network components. Manoeuvre, offensive support, or offensive air support capabilities may be employed to destroy computer network components such as data centers, signals nodes, and command posts using kinetic weapon effects.

3.1.5 Blending

It is important to note that attackers are likely to employ any combination of the above mentioned attacks in a single operation. They may choose to do so to provide a synergistic operational effect or the sequential use may be required to achieve the operational aim. A sequential blending of attacks may enable an attacker to escalate their access level and thus more deeply penetrate a targeted computer network, while a simultaneous combination may achieve a greater disruption of the target network. Likewise the combination of cyber and physical capabilities may achieve greater effect than employing each in isolation.

3.2 Attack Vectors

An attack vector is an avenue or tool that an attacker uses to gain access to a target system or network in order to launch his attacks [21]. Much like disease vectors, attack vectors act as carriers, in this case for malicious code and other activities designed to cause harm to a computer system. As discussed in the previous section, many cyber attacks depend on some level of access to the target system. This means that the attack mechanism must somehow be delivered to the target system. These delivery methods are described in Section 3.2.1. Additionally, there are delivery tools, as described in Section 3.2.2, which often do not require much control from the attacker but can spread and infect other computers by themselves or are spread by tricking the user into downloading them. All of these attack vectors can also be considered as delivery vehicles for some of the attacks previously discussed.

3.2.1 Delivery Methods

The delivery mechanisms described in this section require some level of effort from the adversary in order to set up and launch an attack. These mechanisms are often used to conduct attacks but can also be used as a carrier for the delivery tools described in Section 3.2.2 below.

- Email Attachments: The most classic and commonly known method of delivering malicious code is through email attachments. Attachments make a simple, effective attack vector designed to install malicious code on the recipient's computer as soon as they are opened. The code could be a virus, Trojan-horse, spyware or any other kind of malware. For example, the emails can come from someone in their contacts list who is already infected, or the individual can be spammed using a commonly known company name such a hotels.com with a bogus malicious attachment said to contain their most recent hotel reservation.

- Social Engineering: A tactic that uses lies and manipulation to trick people into revealing their personal information such as their username and password. Email messages can be an effective vehicle for this sort of deception. The adversary gathers freely available information and tries to entice the target to give away bits of information that can be put together to provide them with enough information to either impersonate someone the target trusts or build a relationship with the target strong enough to entice them to visit an infected site or open an infected attachment [28].
- Websites: Malicious web pages can be used to launch attacks. If an unsuspecting individual visits a malicious web page, he can possibly make his systems or networks vulnerable. Malicious downloads may occur by simply visiting web pages that contain malicious web components. File sharing websites are often broken into and download files can be replaced with files containing malware. Insufficiently secured web components also offer attack surfaces susceptible to malicious attacks such as Structured Query Language (SQL) injection and cross-site scripting, where the adversary manipulates the database queries to include malicious code [21].
- Saboteur: An adversary saboteur may infiltrate physical security and gain logical access, either user or administrator privileges, to a terminal on site, in order to install malicious software or hardware. In this instance, the saboteur will either require stolen user/administrator login credentials, or access to a terminal that is currently logged on and unlocked. Alternately, they may entice or coerce personnel with network access to install malicious software, or infect a portable storage device belonging to a person with access so that they unwittingly deliver such software. Also, theft or capture of a mobile terminal, such as a Notebook computer or a vehicle mounted Command and Control system, may offer a similar opportunity. Furthermore, covert installation of hardware at an intermediate point on transmission cables may offer adversaries the ability to eavesdrop on network traffic, keylogging, or even provide a point of access to that network [23].
- IP Address Spoofing: Used to remain anonymous or to redirect blame during an attack. To do this, an attacker changes his IP address to conceal his identity or to impersonate another computer system. When a user sends packets of data into the internet, routers forward the packets to their destination often without checking the validity of the packets' source addresses. An attacker can misuse this by changing the packet's source address to pretend to be another computer [23].

3.2.2 Delivery Tools

The delivery tools described in this section differ from the methods described in the previous section as they often do not require much control from the attacker. They can spread and infect other computers by themselves (self-propagate) or are spread by deceiving the user into downloading them.

- Trojan Horses: A Trojan Horse program, or Trojan, is a program that performs actions which are unknown to and/or unauthorized by the user. It is a program which offers legitimate and useful functionality in order to entice a computer user to download and install it. However, the actual purpose of the program is to install harmful code to the user's computer. The capabilities of Trojans are almost limitless. Some are purely destructive which crash computer systems and/or destroy data, others are used to download adware or spyware, and some can even create backdoors [23][29] .

- Viruses: A computer virus is a program designed to infect a computer, and replicate or copy itself by using a machine's resources without the owner's knowledge and/or permission. Like real life viruses that attack and fuse their DNA with other cells, computer viruses attack legitimate computer programs and fuse into their code. The virus has the same privileges as the software it infects. A virus may also include a payload, or specific actions it performs on the computer that are usually malicious and damaging [23][30].

- Worms: A computer worm is a computer program that self-propagates across a network by exploiting security or policy flaws in widely-used services. Unlike a computer virus, user interaction is not necessary to spread a worm. A worm may include a payload, but this is not a defining feature. A worm's defining characteristic is its need to replicate, or spread copies of itself. A worm is usually categorized based on the vector it uses to propagate, such as via e-mail, chat channels, peer-to-peer networks, etc. Worms used to be considered more benign than Trojans and viruses, as they didn't usually contain malicious payloads. Instead, their negative impact was usually limited to degrading the network itself. More recently, worms are more and more designed to include malicious payloads, and are often as destructive as a Trojan or a virus [23][31].

- Botnets: A 'botnet' is a network of infected computers that can be remotely controlled by an attacker, usually via a command-and-control server. Each infected computer may be known as a bot, a zombie computer, or a zombie. The term 'bot' or 'robot' program refers to a program that can perform repetitive tasks or can act as an 'agent' or user interface for controlling other programs. An attacker, or group of attackers, can harness the collective resources of a botnet to perform major malicious actions, such as stealing data, sending out spam, launching a DDoS attack and much more [32].

- Scareware, Rogues: Scareware, also referred to as Rogue software, essentially pretends to be anti-virus security product software or virus scans. It displays messages to a user that try to convince the user into thinking that their computer has security problems. By convincing the user that their computer is infected, the user will trust the Scareware to remove the fake viruses, but instead it will install real malicious software on the target computer. This is another method used to deliver malware to victim computers using the website delivery method described in Section 3.2.1. Scareware can be pop up advertisements placed on hacked websites or software that users have been tricked into downloading [23]. A variant of scareware is ransomware which disables the functionality of a computer in some way and then the ransomware program displays a message that demands payment to restore functionality [33].

3.3 Adversary Types

Cyber attacks may be initiated for a variety of reasons and by a range of actors of varying skill levels, who have differentiated access to resources. A selection of adversary types are described below, which was mostly drawn from the work conducted at the Lawrence Livermore National Laboratory [17]. For each of the adversary types, they list the corresponding skill level, maliciousness, motivation, and method. Although their work was based on a survey of the literature in the area of cyber crime, by adding the Nation-State type to their list, we obtain a fairly comprehensive list of adversary types.

- Script Kiddies, Newbies, Novices: The least sophisticated of adversaries with limited programming skills, this group is new to cyber attacking and relies on pre-written scripts or "toolkits" to prosecute attacks. While their low skill level limits their threat, the toolkits they utilise are becoming more capable, and their capabilities will grow as a result.
- Hacktivists, Political Activists: This group is motivated by a political cause rather than personal gain. They commonly employ denial of service and defacement attacks against the sites of rival organizations, though they have also been known to employ worms and viruses, and to steal and publish confidential information. Corporate, governmental, and political networks are commonly targeted by this group.
- Cyber Punks, Crashers, Thugs: This group of adversaries are similar in motivation to novices, seeking attention and prestige, but with much greater capabilities. They are able to write basic scripts, and engage in malicious acts such as spamming, defacing, identity theft, and social engineering.
- Insiders, User Malcontents: This group poses a high risk to organisations because of the level of access that is granted to legitimate users of the system. They are most often motivated by revenge, in response to a grievance with their employer. They are capable of inflicting serious damage due to detailed familiarity with their network systems and elevated access privileges. They may attempt to sabotage systems, or disclose sensitive information.
- Coders, Writers: Adversaries in this category create programs that are used by others, particularly novices, and as such, enable more sophisticated attacks by others. They are motivated by power and prestige. Their software can present a serious threat and is often widely proliferated.
- Black Hat Hackers, Professionals, Elite: This group is composed of professional criminals who employ technical hacking skills in criminal enterprises. They are motivated by money and greed. As such, they avoid exposure and prefer to operate with stealth. They are rare, but highly dangerous due to their high level of skill and available resources gained from their exploits. They are often employed by organized crime, and may be described as "guns for hire".
- Cyber Terrorists: This group engages in state-sponsored information technology warfare with attacks to destabilize, disrupt, and destroy the cyber assets and data of an enemy nation or government organization. They are typically well-funded and highly secretive, with extremely high skills and are motivated by ideology.

- Nation-States: These are official actions sanctioned by Foreign Governments, Militaries and Intelligence Services. They are employees of nation-states, and so their motivation reflects the interests of their employers. They are by nature highly skilled, and have access to technical and financial resources, intelligence, physical enabling activity, and physical and legal protection provided by the state. They may seek to destabilize, disrupt, and destroy the cyber assets, data, or even physical installations through cyber or physical means. They may also seek to acquire defence, industrial or diplomatic secrets using network exploitation to further national interests or even military operations.

Figure 4 is a hypothetical chart that depicts the threat posed by the various adversary types and indicates the potential increase in the threat with time. The chart is based on a diagram that was presented at a Black Hat conference in 2003 [34]. Technological advancements increase at an exponential rate and the costs to develop malicious tools decreases. Consequently more sophisticated tools are being developed and made available to the lower skilled adversaries increasing the potential damage they are capable of producing. Additionally, militaries are more openly developing doctrine, tools, tactics and techniques in cyber operations which also increase the threat of Nation States and Cyber Terrorists being involved in cyber activities.

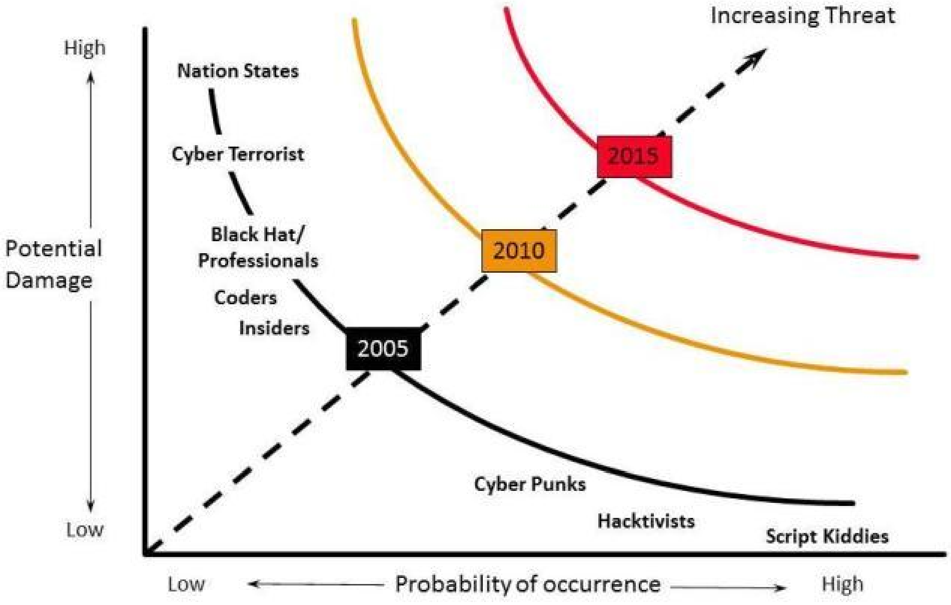

Figure 4: Increasing Threat of Adversary Types (modified from [34])

4 Phase 2: Cyber Effects Characterization

The second phase of the taxonomy development was to characterize the effects that could be achieved by employing the various cyber attacks introduced in Section 3. Cyber attacks typically will adversely impact the critical components of information assurance. Therefore in this section we will explore the effects that cyber attacks may have on information technology infrastructure (ITI) resources and the information that resides on them. In Section 4.1, we start by briefly describing Information Assurance and Information Security. In Section 4.2 we introduce the list of cyber effects and then categorize of the various cyber attacks by the effects they can produce.

4.1 Information Assurance and Information Security

Although information assurance (IA) and information security are often used interchangeably, there is a difference between these terms. The following North Atlantic Treaty Organisation (NATO) definitions will be used to describe these terms.

- Information Assurance: Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities [35].
- Information Security: The protection of information against unauthorized disclosure, transfer, modification or destruction, whether accidental or intentional. Note: Information may exist in the human mind, in document form and in electronic form. Information in the human mind will be protected by the use of appropriate personnel security measures. Information in document form will be protected by the use of appropriate document security measures. Information in electronic form will be protected by the use of appropriate INFOSEC measures [36].

As we are discussing the effects of cyber attacks in this section we are mostly concerned with the electronic form of information security (INFOSEC), which is defined as:

- INFOSEC: The application of security measures to protect information processed, stored or transmitted in communication, information and other electronic systems against loss of confidentiality, integrity or availability (CIA), whether accidental or intentional, and to prevent loss of integrity or availability of the systems themselves [36].

Based on these definitions, INFOSEC can be considered as a subset of IA. INFOSEC focuses more on the technical side (tools and tactics) of information protection. In addition to INFOSEC, IA also includes governance and information and risk management such as certification and accreditation, business continuity planning, and disaster recovery planning. Cyber attacks seek to adversely impact the critical components of IA and INFOSEC, which are often referred to as the CIA Triad and are defined as follows.

- Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information [37].

- Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity [37].
- Availability: Ensuring timely and reliable access to and use of information [37].

4.2 Cyber Effects

In this section, the types of cyber effects that can be produced are discussed as well as which of the cyber attacks described in Section 3 can lead to those effects. There are many ways to describe cyber effects and cyber incidents but there is no current standard. In their paper, Musman et al. [38] proposed a categorical description for cyber attack effects that included six categories. Table 1 describes five of the six categories proposed in [38]. The sixth category was "Unauthorized Use" and it was defined as "an attacker uses system resources for his own purpose and raises the potential for future effects" [38] [39]. In this case Unauthorized Use is more of a means to achieving an effect and therefore in the MACE taxonomy it is not considered a cyber effect. Each effect can affect ITI resources themselves or the information that resides within them. Each effect can also have implications for the operational processes as well as the operational data of the organization under attack [39].

Table 1: Cyber effect categories

Effect	**Description**	**Implication**
Interruption	An attacker causes an ITI asset to become unusable, unavailable, or lost for some specified period of time. Affects the availability component of the CIA triad.	The ITI or information residing within it is unavailable for a specified period of time and the process will be unusable until recovery from the incident.
Modification	An attacker causes a modification of information, data, protocol, or software. Affects the integrity component of the CIA triad.	The information has been altered and as a result the processes that use this information may fail or produce incorrect results.
Degradation	An attacker causes degradation in the performance of an ITI asset. Affects the availability component of the CIA triad.	The rate of information delivery is decreased resulting in the processes involved becoming slowed down.
Fabrication	An attacker causes false information to be inserted into the system. Affects the integrity component of the CIA triad.	False information has been entered in the system and the process could include the insertion of false operational task that may interfere with legitimate operational tasks.
Interception	An attacker causes or takes advantage of information leaked from the system. Affects the confidentiality component of the CIA triad.	The information and/or the process, either via software or hardware, has been captured by the attacker.

The next step is to relate the cyber attacks described in Section 3 to the cyber effects from Table 1. Table 2 serves as a reference for the most significant cyber attacks categorized by the effect they can produce. Each effect may be achieved with different types of attacks, which in turn rely on having different levels of access to the target of the attack. By successfully applying the types of attacks to the categories from Table 1, it is demonstrated that the five categories of effects considered here are sufficient to gain an initial understanding of the types of effects that can be produced in the cyber environment.

Table 2: Cyber attacks categorized by the effect they can produce

Cyber Effect	Attack Type	Minimum Access Required
Interruption	DOS/DDOS	Tier 1 – No Privilege Required
	Stack-based Buffer Overflow	Tier 1 – No Privilege Required
	Malicious Attacks	Tier 2 – Limited Privileges, or Tier 3 – Administrative Privileges
	RootKits/ Kernel Level RootKits	Tier 3 – Administrative Privileges
	Sabotage	Tier 4 – Physical Access
	Electronic Attack	Tier 4 – Physical Access
	Conventional Attack	Tier 4 – Physical Access
Modification	Malicious Attacks	Tier 2 – Limited Privileges, or Tier 3 – Administrative Privileges
	RootKits/ Kernel Level RootKits	Tier 3 – Administrative Privileges
	Sabotage	Tier 4 – Physical Access
	Peripheral Attack	Tier 4 – Physical Access
Degradation	DOS/DDOS	Tier 1 – No Privilege Required
	Stack-based Buffer Overflow	Tier 1 – No Privilege Required
	Scanning	Tier 1 – No Privilege Required
	Malicious Attacks	Tier 2 – Limited Privileges, or Tier 3 – Administrative Privileges
	RootKits/ Kernel Level RootKits	Tier 3 – Administrative Privileges
	Sabotage	Tier 4 – Physical Access
	Electronic Attack	Tier 4 – Physical Access
	Conventional Attack	Tier 4 – Physical Access
Fabrication	Stack-based Buffer Overflow	Tier 1 – No Privilege Required
	Phishing	Tier 1 – No Privilege Required
	Malicious Attacks	Tier 2 – Limited Privileges, or Tier 3 – Administrative Privileges
	RootKits/ Kernel Level RootKits	Tier 3 – Administrative Privileges
	Sabotage	Tier 4 – Physical Access
Interception	Scanning	Tier 1 – No Privilege Required
	Phishing	Tier 1 – No Privilege Required
	Sniffers	Tier 2 – Limited Privileges
	Malicious Attacks	Tier 2 – Limited Privileges, or Tier 3 – Administrative Privileges
	RootKits/ Kernel Level RootKits	Tier 3 – Administrative Privileges
	Spyware/Keyloggers	Tier 3 – Administrative Privileges
	Sabotage	Tier 4 – Physical Access
	Electronic Attack	Tier 4 – Physical Access
	Peripheral Attack	Tier 4 – Physical Access

It should be noted that when considering effects, one must keep in mind the potential for second-order and third-order effects. In the cyber environment there are many interdependencies between the ITI resources. First-order cyber effects are the resulting impacts on ITI systems from direct exploitation of the systems vulnerabilities during the attack. Second-order cyber effects are indirect impacts that the ITI systems experience when network services and communications are lost or restricted due to the attack. Lastly, third-order effects are the overall impacts of the first and second effects that result in loss or degradation of capabilities that are external, yet dependent upon the ITI systems [40].

5 Phase 3: Military Activities Representation

While military operations in the cyber environment are not new, advancements in ITI have blurred the lines between cyber operations and other traditional military activities. In Canada, the Canadian Armed Forces (CAF) defines the Cyber Environment as "The interdependent network of information technology structures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers, as well as the software and data that reside within them" [41]. Although there is still no official definition for Cyber Operations in Canada, it is currently described as *the employment of cyber capabilities where the primary purpose is to achieve objectives in or through the Cyber Environment* [41]. This is based on the United States (US) Department of Defence (DoD) definition in the Memorandum on Joint Terminology for Cyber Operations [42]. Cyber operations can be either offensive or defensive which are currently described in [41] as:

- Defensive Cyber Operations. Cyber operations intended to preserve the ability to utilize friendly cyber capabilities and protect data, software, networks, net-centric capabilities, and other designated systems.
- Offensive Cyber Operations. Cyber operations intended to achieve military objectives in or through the Cyber Environment.

Section 5.1 provides a brief description of offensive cyber operations; Section 5.2 defines the possible military effects within the cyber environment; while Section 5.3 describes how these military effects can be linked to the cyber effects proposed earlier in Section 4.2.

5.1 The Spectrum of Offensive Cyber Operations

Offensive cyber operations as defined in this report and as described in [43] can be considered to include two distinct types of activities: cyber attack, which is destructive by nature and cyber exploitation, which is non-destructive. These two activities are defined as follows:

- Cyber attack: The use of deliberate actions and operations to alter, disrupt, deceive, degrade, or destroy adversary computer systems or networks or the information and (or) programs resident in or transiting these systems or networks. Such effects on adversary systems and networks may also have indirect effects on entities coupled to or reliant on them [43].
- Cyber exploitation: The use of actions and operations to obtain information that would otherwise be kept confidential and is resident on or transiting through an adversary's computer systems or networks [43].

Taking the description of offensive cyber operations one step further, Brown and Tollus [44], propose an interesting view of cyber operations. Rather than establishing strict categories into which cyber activities are sorted, they consider cyber operations along a spectrum of activities. In this view cyber attacks can range from being disruptive and more of a nuisance, to the more destructive and damaging in their effects. Consequently, they consider that there are three broad categories of activities: access operations (where we find cyber exploitation), cyber disruption, and cyber attack. In this case the three categories are defined as follows:

- Enabling (or Access) Operations: Enables other cyber activities by providing entry to an adversary computer system. It includes actions to maintain an access previously gained as well as activities that could be characterized as reconnaissance. The act of gaining or maintaining access, by itself, does not generally affect the system's function or the flow of information. Access operations will generally fall near the left end of the spectrum, but analysis may move them more to the right as the effects they have on the adversary system become more pronounced [44].
- Cyber Disruption: Actions that interrupt the flow of information or the function of information systems without causing physical damage or injury. The greater the effect, the farther it moves along the spectrum, from left to right. Most actions currently defined as computer network attack fall into the category of "cyber disruption" on the spectrum [44].
- Cyber Attack: Actions in the cyber environment whose foreseeable results include damage or destruction of property, or death or injury to persons. Cyber attack falls on the right of the spectrum and moves farther to the right depending on the severity of the attack. To date, the best real-world example of a cyber attack, as defined in this context, is Stuxnet where its intended effect was the destruction of equipment [5][44].

Brown and Tollus make use of a spectrum rather than the strict categorization since although it is possible to describe actions that fit neatly into each category, many operations fall somewhere between the labels, in the margins between these general categories. The spectrum of cyber operations as defined in [44] is depicted in Figure 5 below. The proposed view of classifying cyber operations along a spectrum is quite interesting and merits further investigation for future concept work.

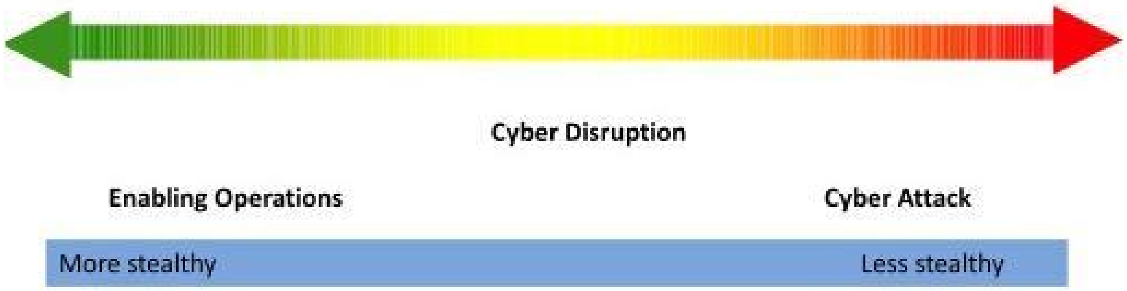

Figure 5: The Spectrum of Cyber Operations as defined in [44]

As indicated earlier, Canada does not have an official definition for Cyber Operations; however there is an existing interim DND/CAF policy for Computer Network Operations (CNO) [45] which by definition is a type of cyber operation. CNO is comprised of, individually or in combination, Computer Network Defence (CND), Computer Network Exploitation (CNE), and Computer Network Attack (CNA). In this case, CNA and CNE would fall under offensive cyber operations. They are defined as follows:

- CNA is a military operation to disrupt, deny, degrade, or destroy information resident in Information Technology Systems (ITS) or the ITS themselves.

- CNE is an intelligence collection activity intended to access, gather data from or control an ITS of an adversary, potential adversary or other Government of Canada approved party.

5.2 Military Activities

Based on the description of offensive cyber operations presented in Section 5.1 and the definition for CNO, the possible military effects in the cyber environment are to deny, degrade, disrupt, or destroy adversary ITI or the information and software residing therein. Also to be considered is digital espionage which is one of the main components of CNE activities. In existing doctrine and current documentation, these military effects are more commonly defined in an information operations or a joint targeting context, and not particularly for the cyber environment. For the purpose of this report, the military effects that can be produced in the cyber environment are defined as follows:

- Deny: To prevent adversary access to the ITI or the information and software residing therein that is needed for effective and timely decision making. Damage done to a function of the system is only temporary, but all aspects of the function are affected [46].
- Degrade: To reduce the effectiveness or efficiency of adversary ITI and information collection efforts or means. Damage done to a function of the system is permanent, but only portions of the function are affected; that is, the function still operates, but not fully [46].
- Disrupt: To break an ITI system or interrupt the flow of information between selected systems. Damage done to a function of the system is only temporary, and only portions of the function are affected [46].
- Destroy: To damage an ITI system or the information and software residing therein so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt. Damage done to the function of the system is permanent, and all aspects of the function are affected [46].
- Digital Espionage: To access personal, commercial, or government information systems and assets for the purpose of theft, misappropriation, destruction, and disinformation for personal or political gain [47].

5.3 Mapping of Cyber Effects to Military Effects

In the second phase of the MACE taxonomy, the various types of cyber effects that can be produced with cyber attacks were characterised (see Table 1 of Section 4.2). In this section, these cyber effects will now be mapped to the possible military effects. The mapping represents which of the cyber effects can be used as a first-order effect to produce the desired military effect. Recall from Section 4.2 that first-order cyber effects are the resulting impact to ITI systems from direct exploitation of the systems' vulnerabilities during the attack. Taking into consideration the definitions for the cyber effects from Section 4.2 and the descriptions of military effects from Section 5.2, the possible mappings in the first-order between the cyber effects and the military effects are presented in Table 3. The mappings were compiled through discussions with subject matter experts by identifying examples of the desired effects [48][49]. If a mapping exists between the two effects, it is represented by a checkmark; otherwise it is denoted by an "X".

Table 3: Mapping of first-order cyber effects to military effects

	Deny	**Degrade**	**Disrupt**	**Destroy**	**Digital Espionage**
Interruption	✓	✗	✓	✗	✗
Modification	✓	✓	✓	✓	✗
Degradation	✗	✓	✓	✗	✗
Fabrication	✓	✓	✗	✗	✓
Interception	✗	✗	✗	✗	✓

Additionally, knowing which cyber effects can produce the desired military effect will also provide the potential cyber attacks that can be applied, based on the information previously provided in Table 2 of Section 4.2. Table 4 provides hypothetical examples of potential cyber attacks or exploitation that could be used to accomplish the desired military effect.

Table 4: Examples of potential cyber attacks or exploitation

Military Effect	**Cyber Effect**	**Example**
Deny	Interruption	Initiating a network flood to cause client software or systems to malfunction so that users are unable to connect to the server [50].
	Modification	Modify server and network configurations, including access controls and routing tables to deny access to a targeted user [23][50].
	Fabrication	A denial of service attack by inserting a large amount of (fabricated) packets on the network with the intent to deny access [48][50].
Degrade	Modification	Modification of the Microsoft Windows registry to stop Windows from functioning correctly and consequently make the targeted system perform much more slowly. If remote registry access is enabled, an attacker may be able to modify configuration settings over the network [50].
	Degradation	Flooding a target with UDP packets consuming network bandwidth and degrading the network access [50].

	Fabrication	A web page could contain any malicious code it wants to execute, if the target browser is vulnerable to it. It could contain a command that is executed as soon as the page is accessed that triggers a botnet to send a DDoS to the target host [43].
Disrupt	Interruption	An attacker that gains physical access can cut a network cable or if using wireless or satellite, jam the signal to interrupt the flow of information [23].
	Modification	An attacker that gains physical access (potentially an insider) can physically reconfigure the network components to redirect network traffic into a black hole which refers to places in the network where incoming traffic is silently discarded and consequently disrupts the flow of information [23][50].
	Degradation	A distributed denial of service attack using a botnet degrades a network to the point where it would collapse under the sheer volume of connections or data [50].
Destroy	Modification	To destroy information, the cyber attacker might seek to delete and permanently erase all data files or reformat and clean all hard disks that it can find [50]. To destroy the system, the attacker might alter the master boot record or slow the fan speed in the BIOS so the system overheats and fails [48].
Digital Espionage	Fabrication	Install malicious code using a phishing attack on a target system that contains code for eavesdropping [48].
	Interception	Using malicious code to compromise a system and install keylogging software that will create logs of what is typed on the keyboard of the attacked system and the time and day it was typed. It can record what program was in use during each keystroke. The attacker could also install a sniffer that can eavesdrop on anything not encrypted that is passed over the compromised system's attached local area network [23].

6 Discussion: Applications of the MACE Taxonomy

In this section we discuss how the MACE taxonomy can be used within cyber security to support military forces. The taxonomy was originally developed to gain a better understanding of the effects achieved by the various cyber attacks. The main purpose was to then simulate these effects for use in simulation in support of training and experimentation [12][51]. This application of the taxonomy is discussed in more detail in Section 6.1. Since the development of the MACE taxonomy and the publication of its Phase 1 approach [22][23], there has been interest to investigate its potential use as the base framework for a cyber threat model. This application of the taxonomy is discussed in Section 6.2 and will be investigated in future work.

6.1 Modeling, Simulation and Experimentation

As described in the previous sections of this paper, cyber attacks come in many types, each with effects that may be observed by network operators and ordinary users. Given military organizations' increased dependency on networks, it is important to explore the potential effects of these attacks through modeling, simulation and experimentation in support of military staff training exercises. Through these methods, we may begin to understand the effects that cyber attacks may have on military commanders' decision-making capabilities and thus on mission effectiveness.

A full simulation of a cyber attack would require a red team (opposing force) to attack the exercise networks and systems, which would prove to be expensive. While this type of simulation would be useful to train "cyber warriors" to defend the network, in our research project [8] we were more interested in investigating the effects of cyber attacks on a modern command post headquarters [12]. Thus, the simulation can be limited to the effects of the cyber attacks on the systems used by the training or exercise audience. Phase 2 and Phase 3 of the MACE taxonomy was developed to facilitate the process of simulating military desired effects for cyber. Being able to describe how military desired effects can be produced by linking these to the cyber attack types, the delivery method used, and the cyber effect, can facilitate the development of scenario vignettes for use in military exercises and experimentation. In fact, Table 2 developed in Phase 2 of the taxonomy was used as the foundation for the development of a series of cyber events/vignettes for recent CAF experiments and exercises. A total of sixteen scenario events were developed by CAE Integrated Enterprise Solutions, Canada [51]. The scenario events were developed to evenly span the range of cyber effects and attacks presented in Table 2 and in turn provided sufficient variety and realism to present the experiment participants with a cross-section of potential cyber events to address. The CAE developed events supporting the following three CAF experiments and exercises:

- Coalition Attack Guidance Experiment (CAGE) II. CAGE II was the second in an ongoing series of human-in-the-loop hypothesis testing experiments that was conducted 5-16 November 2012 with distributed in situ military participation from Australia, Canada, and the United States. Canadian participation in CAGE II was under the leadership of the Canadian Forces Warfare Centre and involved several organizations from the CAF and the Department of National Defence, including Director General Cyber. [52]

- JOINTEX 2013. JOINTEX 2013 was the first in a series of nation-wide joint training and readiness events designed to change how the Canadian Armed Forces train, develop and learn to prepare for future operations. Intended to be conducted in five stages, JOINTEX began in 2010 and the final stage concluded on 8 June 2013. It was conceived to train a Canadian-led Combined Joint Inter-Agency Task Force Headquarters in the planning and conduct of coalition full-spectrum operations in a joint, inter-agency, multinational and public environment [53].
- Determine Dragon 13 (DD13). DD13 is a Canadian Joint Operations Command led exercise designed to confirm its ability to plan and conduct bi-lateral defence operations within the North American continent. The exercise was conducted 28 October to 4 November 2013 [54].

6.2 Cyber Threat Model

The MACE taxonomy can also be applied as a potential component of a cyber threat model. The concise description of the mechanisms of cyber attacks is a key element in planning and executing defences against such attacks. Describing an adversary's objective in terms of the six categories of the MACE taxonomy could provide the first step required in describing a cyber threat. Overlaying such a threat description with a framework like the MITRE Corporations' Cyber Prep methodology [20] or Sandia National Laboratories' Operational Threat Assessment (OTA) methodology [21] could potentially provide an effective threat model. These two frameworks provide metrics and models to characterize a cyber threat:

- The Cyber Prep methodology provides an organization a framework to characterize its desired level of preparedness against cyber adversaries, to establish goals and strategies and to incorporate the phased implementation of security measures and the evolution of governance structures and processes into its strategic planning [20].
- The OTA methodology is based on a generic threat matrix which provides a framework for ordering a set of relevant threat metrics and for describing malicious cyber threats to systems. The purpose of the matrix is to identify attributes that could help an analyst characterize threats based on their overall capabilities and to categorize them into a common vocabulary [21].

The development of a cyber threat framework and model along with the potential application of the MACE taxonomy will be investigated further in future work within the Security and Defence Metrics work stream of the Cyber Decision Making and Response project within the DRDC Cyber Science and Technology Program [55].

7 Conclusion

This report proposed a taxonomy for military activities and cyber effects that will provide a common framework for military cyber operators and defenders to assist in the understanding of the threats they face. The MACE taxonomy was developed in three phases. The first phase classified the cyber attacks based on the level of access that the attacker required to launch the attack. It described the types of adversaries that would be involved in a cyber attack and described various delivery mechanisms. The second phase characterised the cyber effects and then categorized the various cyber attacks by the effects they can produce. The third and final phase brought in the military context. It represented the military activities within the cyber environment and describes the desired effects from a military perspective and how these relate to the cyber effects and subsequently the cyber attacks. The resulting taxonomy classifies cyber attacks based on the level of access required to launch the attack, the cyber effects it can produce and the military activities it can be used for. It consists of six main categories: Attack Types, Levels of Access, Attack Vectors, Adversary Types, Cyber Effects, and Military Activities.

The taxonomy was originally developed to gain a better understanding of the effects achieved by the various cyber attacks in order to then simulate these effects for use in modeling, simulation and experimentation. Portions of this taxonomy have been applied to create a series of cyber scenario events/vignettes that involve simulating the cyber effects desired for use in military experiments and exercises. In future work we will investigate the potential extension of applying the taxonomy as part of a cyber threat model and the assessment of an organization’s cyber defence posture.

References

[1] Public Safety Canada, *Canada's Cyber Security Strategy*, Government of Canada, 2010.

[2] Lesk, M., *The New Front Line: Estonia Under Cyberassault*, IEEE Security & Privacy Volume 5, Issue 4, pp. 76-79, July/August 2007.

[3] Markoff, J., *Before the gunfire, cyber attacks*, The new York Times, August 13, 2008.

[4] Diebert, R., Rohozinski, R., *Tracking GhostNet: Investigating a Cyber Espionage Network*, Information Warfare Monitor, JR02-2009, March 2009.

[5] Falliere, N., Murchu, L., Chien, E., *W32.Stuxnet Dossier, Version 1.4*, Semantec Security Response, Semantec Corporation, February 2011.

[6] Department of National Defence, *Canada First Defence Strategy*, Government of Canada, 2008.

[7] Weston, G., *Foreign hackers attack Canadian government*, CBC News, February 16, 2011.

[8] Bernier, M., Leblanc, S.P., *Applied Research Project Proposal: Modeling and Simulation of Cyber Effects and Capabilities for C2*, Presentation to DRDC Partner Group 5 Thrust b, 22 October 2009.

[9] Department of National Defence, *Defence Terminology Bank, Record 31986: taxonomy*, Government of Canada, accessed Sept 26, 2012.

[10] Bruno, D., Richmond, H., The Truth About Taxonomies, Information Management Journal, March/April 2003, pp 45-53.

[11] Howard, J.D., Longstaff, T.A., A Common Language for Computer Security Incidents, SANDIA REPORT SAND2012-2427, Sandia National Laboratories, October 1998.

[12] Chapman, I.M., Leblanc, S.P., Partington, A., Taxonomy of Cyber Attacks and Simulation of their Effects, DRDC CORA SL2011-07, Proceedings of the Military Modeling & Simulation Symposium (MMS), April 2011.

[13] Weaver, N., Paxson, V., Staniford, S., and Cunningham, R., *A Taxonomy of Computer Worms*, Proceedings of the 2003 workshop on Rapid malcode (WORM 2003), pp 11-18, October 2003.

[14] Mirkovic, J., Reiher, P., *A taxonomy of DDOS attacks and DDOS defence mechanisms*, ACM SIGCOMM Computer Communication Review, 34(2), April 2004.

[15] Kotapati, K., Liu, P., Sun, Y., and LaPorta, T., *A Taxonomy of Cyber Attacks on 3G Networks*, Technical Report NAS-TR-0021-2005, Network and Security Research Center, Department of Computer Science and Engineering, Pennsylvania State University, University Park, PA, USA, January 2005.

[16] Hansman, S. and Hunt, R., *A taxonomy of network and computer attacks*, Computers and Security 24(1), pp. 31-43, 2005.

[17] Meyers, C. Powers, S., Faissol, D., Taxonomies of Cyber Adversaries and Attacks: a Survey of Incidents and Approaches, Technical Report LLNL-TR-419041, Lawrence Livermore National Laboratory, April 2009.

[18] Simmons, C., Ellis, C., Shiva, S., Dasgupta, D., Wu, Q., *AVOIDIT : A cyber attack taxonomy*, Department of Computer Science, University of Memphis, 2009, http://issrl.cs.memphis.edu/files/papers/CyberAttackTaxonomy_IEEE_Mag.pdf, accessed July 25, 2013.

[19] Applegate, S., Stavrou, A., *Towards a cyber conflict taxonomy*, Proceedings of the 5th International Conference on Cyber Conflict (CyCon2013), K. Podins, J. Stinissen, M. Maybaum (Eds.), NATO CCD COE Publications, Tallinn, June 2013.

[20] Bodeau, D.J., Graubart, R.D., Fabius-Greene, J*., Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels*, Proceedings of the 2010 IEEE International Conference on Social Computing, pp. 1147-1152, August 2010.

[21] Mateski, M., Trevino, C.M., Veitch, C.K., Michalski, J., Harris, J.M., Maruoka, S., Frye, J., *Cyber Threat Metrics*, SANDIA REPORT SAND98-8667, Sandia National Laboratories, March 2012.

[22] Partington, A., Leblanc S.P., *A Taxonomy of Cyber Attacks for Use in Computer Network Attack Modelling and Simulation*, ECE-2010-03, Royal Military College of Canada Computer Security Laboratory, 18 December 2010.

[23] Partington, A., Morton, B., Leblanc S.P., *A Taxonomy of Cyber Attacks for Use in Computer Network Attack Modelling and Simulation Version 2.0*, ECE-2011-01, Royal Military College of Canada Computer Security Laboratory, 22 August 2011.

[24] Verdasys, *Cyber Attack Defense - A Kill Chain Strategy*, Verdasys White Paper, 2013, https://www.verdasys.com/resources/#White%20Papers, accessed 23 August 2013.

[25] Hutchins, E., Cloppert, M., Amin, M., *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion kill Chains*, Lockheed Martin Corporation White Paper, http://www.lockheedmartin.ca/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf, accessed 23 August 2013.

[26] Nice, S., The hacker's guide to website security, 5 May 2010, http://www.techradar.com/news/internet/the-hackers-guide-to-website-security-687153/1#articleContent, accessed 29 January 2013.

[27] Smith, S. Harrison, J., *Rootkits*, Semantec Security Response, Semantec Corporation, 2012.

[28] Goodchild, J., *Social Engineering: The Basics*, CSO Security and Risk, 20 December 2012, http://www.csoonline.com/article/514063/social-engineering-the-basics, accessed 22 October 2013.

[29] F-Secure, *About Trojans*, http://www.f-secure.com/en/web/labs_global/articles/about_trojans, accessed 7 March 2013.

[30] F-Secure, *About Viruses*, http://www.f-secure.com/en/web/labs_global/articles/about_viruses, accessed 7 March 2013.

[31] F-Secure, *About Worms*, http://www.f-secure.com/en/web/labs_global/articles/about_worms, accessed 7 March 2013.

[32] F-Secure, *About Botnets*, http://www.f-secure.com/en/web/labs_global/articles/about_botnets, accessed 7 March 2013.

[33] O'Gorman, G., McDonald, G., *Ransomware: A Growing Menace*, Semantec Security Response, Semantec Corporation, 2012.

[34] Sachs, M., Parker, T., Shaw, E., Miller, T., *Adversary Characterization and Scoring Systems*, Black Hat Federal 2003, http://www.blackhat.com/presentations/bh-usa-03/bh-us-03-parker.pdf, accessed 30 October 2013.

[35] Combined Communications Electronics Board, *Information Assurance for Allied Communications and Information Systems*, ACP 122(F), December 2008.

[36] North Atlantic Treaty Organization*, NATO Glossary of Communication and Information Systems Terms and Definitions*, AAP31.

[37] National Institute of Standards and Technology, Glossary of Key Information Security Terms, NIST IR 7298 Revision 1, US Department of Commerce, February 2011.

[38] Musman, S., Temin, A., Tanner, M., Fox, D. and Pridemore, B., *Evaluating the Impact of Cyber Attacks on Missions*, In Armistead, E. and Cowan, E. (eds.), Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, Ohio, pp. 446-456, April 2010.

[39] Musman, S., Tanner, M., Temin, A., Elsaesser, E. and Loren, L., *Computing the Impact of Cyber Attacks on Complex Missions*, In Proceedings of the IEEE International Systems Conference (SysCon), Montreal, Quebec, pp. 46-51, April 2011.

[40] Powell, S., *Methodology for Cyber Effects Prediction*, Black Hat DC 20120, 22 January 2010.

[41] Chief of Force Development, *CAF Cyber Operations Primer - Draft V0.9*, Department of National Defence, Canada, 1 July 2013.

[42] Cartwright, J., *Memorandum on Joint Terminology for Cyberspace Operations*, , United States Department of Defense, Washington, DC.

[43] Lin, H., *Offensive Cyber Operations and the Use of Force* , Journal of National Security Law & Policy, Vol. 4:63, August 2010.

[44] Brown, G., Tollus, O., *On the Spectrum of Cyberspace Operations*, Small Wars Journal, 11 December 2012.

[45] Chief of Defence Staff, *Interim Department of National Defence and Canadian Forces Policy on Canadian Forces Computer Network Operations* (Secret//Rel AUSCANZUKUS), Department of National Defence, Canada, October 2012.

[46] United States Joint Forces Command, *Joint Fires and Targeting Handbook*, 19 October 2007.

[47] Nichols, R., Ryan, D., and Ryan, J., *Defending Your Digital Assets Against Hackers, Crackers, Spies, and Thieves*, McGraw-Hill, United States, 5 January 2000.

[48] Cyber and military effects mapping, private communication, Joanne Treurniet, May 1-2, 2013.

[49] SME advice on cyber effects mapping, private communication, Capt. Desmond Gosse, May 2-5, 2013.

[50] Trusted Information Sharing Network for Critical Infrastructure Protection, *Managing Denial of Service (DoS) Attacks*, Attorney-General's Department, Government of Australia, June 2006.

[51] Miller, J., *Coalition Attack Guidance Experiment (CAGE) II Event and Inject Development*, DRDC CORA CR2013-025, Defence Research and Development Canada, March 2013.

[52] Canadian Forces Warfare Centre, *Coalition Attack Guidance Experiment (CAGE II) Canadian Experiment Instruction*, DND, Ottawa, 9 October 2012.

[53] Canadian Joint Operations Command, *JOINTEX 2013*, CJOC BG 2013-001, http://www.cjoc.forces.gc.ca/ex/jointex/index-eng.asp, accessed July 24, 2013.

[54] Canada Command, *Canada Command Business Plan Fiscal Year 2012/2013*, 12 January 2012.

[55] Lefebvre, J., "*Cyber S&T Program Decision Brief to DG Cyber*", Defence Research and Development Canada, 1 March 2013.

List of symbols/abbreviations/acronyms/initialisms

[Enter list here, if applicable. If not, delete the page.]

ARP	Applied Research Project
CAF	Canadian Armed Forces
CAGE II	Coalition Attack Guidance Experiment II
CIA	Confidentiality, Integrity, Availability
CNA	Computer Network Attack
CND	Computer Network Defence
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CORA	Centre for Operational Research and Analysis
DD13	Determine Dragon 13
DND	Department of National Defence
DNS	Domain Name System
DoD	Department of Defense
DDOS	Distributed Denial of Service
DOS	Denial of Service
DRDC	Defence Research & Development Canada
DRDKIM	Director Research and Development Knowledge and Information Management
EM	Electromagnetic
FTP	File Transfer Protocol
IA	Information Assurance
INFOSEC	Information Security
IP	Internet Protocol
ITI	Information Technology Infrastructure
ITS	Information Technology Systems
LAN	Local Area Network
MACE	Military Activities and Cyber Effects
NATO	North Atlantic Treaty Organisation

OR	Operational Research
OTA	Operational Threat Assessment
R&D	Research & Development
RMCC	Royal Military College of Canada
SQL	Structured Query Language
SSH	Secure Shell
TM	Technical Memorandum
US	United States
USB	Universal Service Bus
Wi-Fi	Wireless

This page intentionally left blank.

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (The name and address of the organization preparing the document. Organizations for whom the document was prepared, e.g. Centre sponsoring a contractor's report, or tasking agency, are entered in section 8.) Defence R&D Canada – CORA 101 Colonel By Drive Ottawa, Ontario K1A 0K2	2. SECURITY CLASSIFICATION (Overall security classification of the document including special warning terms if applicable.) UNCLASSIFIED (NON-CONTROLLED GOODS) DMC: A REVIEW: GCEC April 2011

3. TITLE (The complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S, C or U) in parentheses after the title.)

Military Activities and Cyber Effects (MACE) Taxonomy:

4. AUTHORS (last name, followed by initials – ranks, titles, etc. not to be used)

Bernier, M.

5. DATE OF PUBLICATION (Month and year of publication of document.) December 2013	6a. NO. OF PAGES (Total containing information, including Annexes, Appendices, etc.) 54	6b. NO. OF REFS (Total cited in document.) 55

7. DESCRIPTIVE NOTES (The category of the document, e.g. technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered.)

Technical Memorandum

8. SPONSORING ACTIVITY (The name of the department project office or laboratory sponsoring the research and development – include address.)

Defence R&D Canada – CORA
101 Colonel By Drive
Ottawa, Ontario K1A 0K2

9a. PROJECT OR GRANT NO. (If appropriate, the applicable research and development project or grant number under which the document was written. Please specify whether project or grant.) DRDC ARP 15bh	9b. CONTRACT NO. (If appropriate, the applicable number under which the document was written.)
10a. ORIGINATOR'S DOCUMENT NUMBER (The official document number by which the document is identified by the originating activity. This number must be unique to this document.) DRDC CORA TM 2013-226	10b. OTHER DOCUMENT NO(s). (Any other numbers which may be assigned this document either by the originator or by the sponsor.)

11. DOCUMENT AVAILABILITY (Any limitations on further dissemination of the document, other than those imposed by security classification.)

Unlimited

12. DOCUMENT ANNOUNCEMENT (Any limitation to the bibliographic announcement of this document. This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in (11) is possible, a wider announcement audience may be selected.))

Unlimited

13. ABSTRACT (A brief and factual summary of the document. It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified. Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), (R), or (U). It is not necessary to include here abstracts in both official languages unless the text is bilingual.)

Malicious cyber activities are continually growing both in number and in complexity. There are many types of cyber attacks that exist and each can produce a range of effects. In order to facilitate an improved shared understanding of threats in the cyber environment among military operators, we propose in this report a taxonomy for Military Activities and Cyber Effects (MACE). The MACE taxonomy was originally developed as the foundation for the modeling, simulation and experimentation of cyber attacks and the effects they can produce, but was then expanded to describe the linkages to military activities and their desired effects. It consists of the following six categories: Attack Types, Levels of Access, Attack Vectors, Adversary Types, Cyber Effects, and Military Activities. Together these can provide the underlying structure for the development of a threat model or can easily provide the details required to develop scenario vignettes for cyber related experiments and exercises. This report describes in detail the six categories of the taxonomy.

Le nombre et la complexité des cyberattaques augmentent sans cesse. Or, il existe plusieurs types de cyberattaques, donc chacune peut entraîner plusieurs conséquences. Afin de favoriser une meilleure compréhension commune des cybermenaces dans les milieux militaires, le présent rapport propose une taxonomie des activités militaires et des conséquences informatiques (AMCI). Originellement développée pour modéliser et simuler les cyberattaques et leurs conséquences ainsi que faire des expériences à ce propos, la taxonomie AMCI a ensuite été amplifiée afin de décrire les liens avec les activités militaires et les effets voulus de celles-ci. Elle compte six grandes catégories : types d’attaques, degrés d’accès, vecteurs d’attaque, types d’adversaires, conséquences informatiques et activités militaires. Dans leur ensemble, ces catégories peuvent former la structure sous-jacente au développement d’un modèle de menaces, et elles peuvent donner rapidement les détails nécessaires au développement de scénarios destinés à des expériences et exercices touchant les cybermenaces. Le rapport décrit en détail les six catégories de cette taxonomie.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (Technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document. They should be selected so that no security classification is required. Identifiers, such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selected from a published thesaurus, e.g. Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus identified. If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title.)

Cyber Effects, Cyber Attacks, Taxonomy, Military Activities, Military Effects