On the Probability of Predicting and Mapping Traditional Warfare Measurements to the Cyber Warfare Domain

Marthie Grobler, Ignus Swart

On the Probability of Predicting and Mapping Traditional Warfare Measurements to the Cyber Warfare Domain

Prof Marthie Grobler[1, 2], and Ignus Swart[1]

[1] Council for Scientific and Industrial Research, Pretoria, South Africa
[2] University of Johannesburg, Johannesburg, South Africa

mgrobler1@csir.co.za, iswart@csir.co.za

Abstract: Cyber warfare is a contentious topic, with no agreement on whether this is a real possibility or an unrealistic extension of the physical battlefield. This article will not debate the validity and legality of the concept of cyber warfare, but will assume its existence based on prior research. To that end the article will examine research available on traditional warfare causes, elements and measurement techniques. This is done to examine the possibility of mapping traditional warfare measurements to cyber warfare. This article aims to provide evidence towards the probability of predicting and mapping traditional warfare measurements to the cyber warfare domain. Currently the only way of cyber warfare measurement is located in traditional information security techniques, but these measurements often do not adequately describe the extent of the cyber domain. Therefore, this paper aims to identify a set of criteria to aid in the prediction of cyber warfare probability.

Keywords: cyber warfare, metrics, prediction, probability, traditional warfare

1 Introduction

This article will not debate the validity and legality of the concept of cyber warfare, but will assume its existence based on prior research performed by Heickerö [10] and Liles, Rogers, Dietz and Larson [14]. To that end this article will examine the history of research available on traditional warfare pre-requisites and measurement techniques. This is done to examine the possibility of mapping traditional warfare measurements to cyber warfare.

Currently the only way of measurement is located in traditional information security techniques. While applicable, the measurements do not adequately describe loss, posture or any of the pre-requisites found in traditional warfare. This article aims to provide evidence towards the probability of predicting and mapping traditional warfare measurements to the cyber warfare domain.

1 Predicting Traditional Warfare

There have been many attempts to predict and prevent traditional warfare. Unfortunately, many of the causes identified as precursors for warfare cannot be manipulated towards predicting warfare [23]. This section looks at the accepted causes of traditional warfare and builds on these causes as metrics for traditional warfare.

1.1 Causes of Traditional Warfare

Research by Van Evera [23] and Schelling (in [23]) focus on the causes of war that relates to the character and distribution of national power. The hypotheses of these works are that warfare is more likely when:

1. **Nation states fall prey to false optimism about the outcome of war.** This occurs when nation states exaggerate their own chances of winning crises and wars, or when they underestimate the cost of war. For example, when nation states are so sure that their military force is stronger than an opponent, they may be less risk averse and take bigger risks.
2. **The advantage lies with the first side to mobilise the attack.** This occurs when nation states launch pre-emptive attacks to prevent their opponents from attacking first. This has a negative impact on diplomacy, since nation states tend to conceal their capabilities and grievances for fear that open displays of strength or grievance could trigger another nation states' pre-emptive attack. For example, Hitler's 1940 attack on Norway was purely a move to advance the Germans' position in the war.
3. **The power of nation states fluctuates sharply, with large windows of opportunity and vulnerability.** Fluctuations in power tempt nation states to launch preventive attacks and rush into war sooner if they predict their own vulnerability to grow in the future. In some cases diplomacy becomes hurried in an attempt to resolve disputes before power wanes, often resulting in less valuable diplomatic agreements or a complete loss of diplomacy. For example, in the 16th century the weaker Dutch nation revolted against the Spanish due to their imminent subjugation to Spanish rule.
4. **Resources are cumulative.** This occurs when the control of resources enables a nation state to protect or acquire other resources that can be readily used to seize more resources. It is found that cumulative resources often predict further gains or losses. Therefore, the greater the cumulativity of conquerable resources, the greater the risk of war. This was illustrated as far back as the Roman wars that forced tax collection from conquered nations to continue the war effort.
5. **Conquest is easy.** Easy conquest is a master cause of other potent causes of war, raising all the risks they pose. This was clearly demonstrated when China and the League of Nations did nothing to stop the invasion of Manchuria by Japan in 1932.

These causes of war will form the foundation of this research study, and will serve as the main metrics to measure damage and potential loss due to warfare.

1.2 Traditional Warfare Elements

For the purpose of this paper, war can be defined as a state of armed conflict between different countries or different groups within an environment. There are a number of theories about the elements that comprise traditional warfare. For the purpose of this research study, the thinking of Clausewitz will be followed. Although not exhaustive, the authors felt that Clausewitz's thinking is most representative and applicable to the cyber domain. Clausewitz (in [19]) believed that an offensive act has to meet certain criteria in order to qualify as an act of war:

- **It has to have the potential to be lethal.** If an act cannot be considered as potentially violent, it is not an act of war. A real act of war is always lethal, for at least some participants on at least one side. Although none of the hypotheses listed in Section 1.1 mentions violence, this element links to all the causes of warfare in that the offending nation state aims to gain control over the defending nation state, thereby debilitating the defending nation states. This debilitation can take the form of death of soldiers or the destruction of the defending nation state's resources.
- **It has to be instrumental.** The act of war has to have a means and an end. Generally, physical violence or the threat of force is the means. The end is to force the enemy to accept the offender's will, or to render one opponent defenceless. In terms of the hypotheses listed in Section 1.1, causes 2, 3 and 4 addresses the means of war, whilst cause 1 and 5 addresses the end of war.
- **It has to be political.** While the motivation for war might include a variety of factors, ultimately it has to be government sanctioned and can thus be considered as political. Therefore, war's larger purpose is always political in nature. It transcends the use of force and is never an isolated act. Therefore, a political entity or a representative of a political entity has to have an articulated intention that has to be transmitted to the adversary at some point during the confrontation. In terms of the hypotheses listed as causes for traditional warfare, cause 3 relates to politics.

1.3 Metrics for Traditional Warfare

The hypotheses in Section 1.1 and the supporting elements in Section 1.2 can be concatenated into five factors, considered as metrics for predicting traditional warfare. These five factors are presented as the following formula for predicting the possibility of traditional warfare:

Possibility of traditional warfare = Nation state political power fluctuations
AND Potential for lethality
AND ((False optimism
AND Offending nation state advantage)
OR Easy conquest)

In order to predict the possibility of traditional warfare, three conditions need to be met. These conditions are:

- **Condition 1:** The offending nation state needs to have political power fluctuations present, including a political purpose and non-isolated events.

- **Condition 2:** The potential for lethality needs to be present.
- **Condition 3:** This condition is complex with three sub conditions (either the first two sub conditions need to be true, or the third sub condition needs to be true):

– **Sub condition 1:** The offending nation state needs to have false optimism regarding its own capability.
– **Sub condition 2:** The offending nation state needs to believe that their actions will lead to an advantageous position, often due to cumulative resources.
– **Sub condition 3:** The offending nation state needs to believe that the war will be an easy conquest, referring to the target's capability.

The next section aims to apply the formula for predicting the possibility of traditional warfare to cyber warfare, in an attempt to identify a set of criteria specific to the cyber domain to aid in the prediction of cyber warfare probability.

2 Defining Cyber Warfare

Cyber warfare is a contentious topic, with no agreement on whether this is a real possibility or an unrealistic extension of the physical battlefield. Regardless of this ongoing debate, however, the cyber domain is playing a definite role in warfare. Whether it is a full blown Denial of Service attack, hacking attempt or the use of secured online communication to discuss strategy and tactics, technology has a definite place in the warfare domain. Accordingly, cyber warfare can be seen as both offensive and defensive operations against information resources, conducted because of the potential value that information resources have to people [24]. This section will look at the definition of cyber warfare, before mapping the formula for predicting the possibility of traditional warfare to cyber warfare.

Legally, there is no concept such as cyber war. The United Nations Charter specifies when a nation state can use force in self-defence against an act of aggression, but this refers only to armed conflict [4], see Condition 1. To complicate this further, there is no such thing as a digital only war. It is therefore not accurate to assume that cyber war is a war fought only in the cyber domain, only between cyber elements [8]. *"Although cyberspace is a man-made domain, it has become just as critical to military operations as land, sea, air and space"* [19]. Therefore, it is understandable that some entities claim that cyber war is the fifth domain of warfare (after land, sea, air and space) [22]. For the purpose of this paper, the Oxford Dictionaries [17] definition of cyber war is adopted:

The use of computer technology to disrupt the activities of a state or organisation, especially the deliberate attacking of communication systems by another state or organisation.

The impact that cyber warfare has, however, is indisputable. Already in 1995 the following statement were made by Chinese Major General Wang Pufeng: "*In the near future, information warfare will control the form and future of war. We recognize this developmental trend of information warfare and see it as a driving force in the modernization of China's military and combat readiness. This trend will be highly critical to achieving victory in future wars."* [13].

2.1 Acts of Cyber aAggression

As in traditional warfare, each war consists of several battles, i.e. no attack is isolated (refer to Condition 1). In the cyber domain, these battles are referred to as acts of cyber aggression. Currently, there is no international treaty in place that establishes a legal definition for an act of cyber aggression. However, research by Carr [4] reasons that these acts include:

- Cyber attacks against government or critical civilian websites or network without accompanying military force.
- Cyber attacks against government or critical civilian websites or network with accompanying military force.
- Cyber attacks against internal political opponents.
- Cyber intrusions intro critical infrastructure and networks.
- Acts of cyber espionage.

While a variety of factors can be added to the list, it can be argued that the categories listed by Carr is fairly comprehensive. For example, the global worker is irrelevant since any action from the worker would fall into the categories defined by Carr.

According to research done by Filiol [8], acts of cyber aggression have five definite characteristics. Although these characteristics are generic enough to be applicable to any cyber related act, these characteristics form the foundation of the discussion of cyber aggression..

- **Dematerialisation.** Anonymity is a key factor in cyber war since true anonymity is a sought after skill in itself. By achieving anonymity, the attackers actually showcase how easily they can perform an action without detection. Therefore, the true origin of the attack must remain hidden, and it must be possible to wrongly frame an innocent party as the perpetrator of the attack. Although the potential level of anonymity may give attacking nations the courage to take appropriate risk in an attack, the anonymity will not get the message of superior cyber-warfare capability across. Therefore, from a military perspective, the main interest is to avoid or delay the target reaction by misleading it (refer to Sub conditions 2 and 3).
- **Cancelling time and space limits.** By extending the war domain, this serves as a strong barrier for the attacker. All traditional restrictions are removed from the planned attack, making the potential scope for attack much bigger. Network connections will make it possible to have immediate access from anywhere and at any time (refer to Sub condition 2).
- **Gaining control over time and space, over physical resources.** The aim of war is to gain such control over the physical world in order to use these resources to the maximum benefit of the cyber war's intended outcome (refer to Condition 2 and Sub condition 2).
- **Exploit the complexity, interdependencies of modern systems.** The attacking nation does not have to directly attack the target, but rather attack unsecured targets which have some kind of interdependencies on the actual target. E.g. by attacking transportation facilities, critical infrastructure, etc. not only the government but also the civilians are inconvenienced. The affected civilians will, in turn, put in-

creasing pressure on the originally intended target, the government (refer to Sub condition 3).

- **Exploit generalised intelligence.** The aim is to openly collect a large amount of possible useless or common data and compile in order to have significant and deep knowledge of a given target (refer to Condition 1 and Sub condition 3).

3 The Status of Current Information Security Metrics

To measure information security a holistic approach needs to be followed. In an attempt to organise and structure information security measurements, the MITRE Corporation has defined several key areas that are affected by any measurement in cyber security readiness. Therefore, all the categories in **Error! Reference source not found.** need to be taken into account due to the complexity of information interaction points. As such, it becomes a complicated process to measure all these categories accurately. This often results in false optimism (Sub condition 1) about the status of information security management within a nation state, and the ability of a nation state to protect against potential cyber attacks. In addition, this false optimism can also lead to an easy conquest (Sub condition 3), if a nation state overestimates its own cyber abilities (refer to Section 1.3).

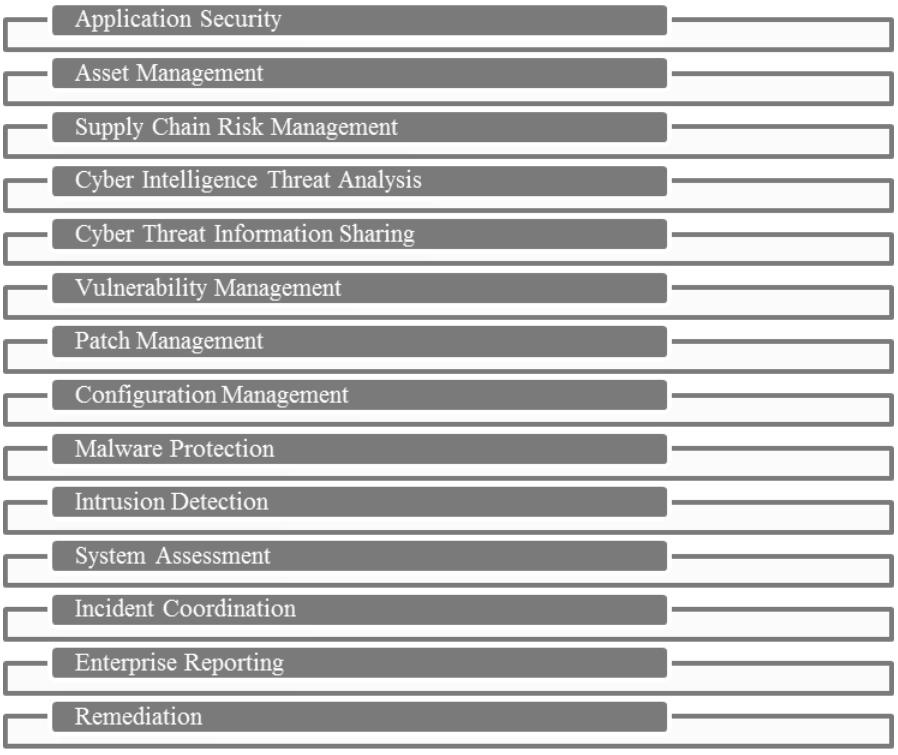

Fig. 1. Categories affecting information security [16]

Metrics for information security currently fall into two areas: high level metrics that assess what a nation is investing in via policy and response teams, and on a more technical side, measurements for the vulnerability of software/devices/services. Both types of metrics can be measured: the high level metrics through research such as the Cyber Readiness Index (CRI) and technical metrics through applying standards such as Common Vulnerability and Exposures (CVEs) to applications/devices/services. Technical difficulties in the measurement of either exist that does not just affect individual nations but is a global area of concern. It is therefore important to distinguish between the two areas of measurement and factor in both, since taking either into account in isolation can lead to incorrect assumptions regarding the state of a nation state's information security posture.

3.1 Cyber Readiness Index

The CRI examined 35 countries that have embraced ICT and the Internet to evaluate each country's maturity and commitment to cyber security across five essential elements. These elements were identified based on where cyber security can be used to protect the value and integrity of previous ICT investments and enable the Internet economy [9]. The five essential elements are:

- **Articulation and publication of a National Cyber Security Strategy.** The country has to have articulated and published a National Cyber Security Strategy that describes the threats to the country and outlines the necessary steps, programmes and initiatives that must be undertaken to address the threat. In fulfilling this element, the country has to address the percentage of Gross Domestic Product (GDP) embraced by the plan, identify commercial-sector entities affected by and responsible for implementation of the plan as well as critical services, and establish continuity of service agreements for each critical service [9]. This element links to Sub conditions 1 and 2.
- **Operational Computer Emergency Response Team (CERT) or Computer Security Incident Response Team (CSIRT).** To facilitate national incident response in the event of natural disasters or man-made disasters that affect critical services and information infrastructures, a CERT/CSIRT should be in place. In fulfilling this element, the country has to publish an incident response plan for emergencies and crises, put in place incident management, resiliency and recovery capabilities for critical services and information infrastructures, and have a network of national contact points for governmental and regulatory bodies [9]. This element links to Sub condition 2.
- **Demonstrate commitment to protect against cyber crime.** The country's involvement with international treaty agreements is assessed by means of treaty ratification. By ratifying a treaty, a country has an obligation and right under international law to uphold its political commitment. In fulfilling this element, the country needs to determine what percentage of GDP is affected by cyber crime, prepare an annual threat assessment to government and critical infrastructure networks, establish criminal offenses under its domestic law for cyber actions against computer systems, networks and computer data, and review existing laws and regulatory

governance mechanisms applicable to cyber crime [9]. This element links to Condition 1 and Sub condition 2.

- **Information sharing mechanism.** An information sharing mechanism needs to be in place to enable the exchange of actionable intelligence/information between government and industry. In fulfilling this element, the country needs to have mechanisms in place for cross-sector incident-information sharing, have a rapid assistance mechanism and have the ability to declassify intelligence information and share it with rest of government and critical industries [9]. This element links to Condition 1.
- **Investment in cyber security research and funding of cyber security initiatives.** The country needs to invest in cyber security basic and applied research (innovation) and be funding cyber security initiatives broadly. In fulfilling this element, the country needs to dedicate a specified percentage of GDP (or government budget) to cyber security research and development, determine the research/production conversion and commercial adoption rate of research programmes, have universities offer a degree program in cyber security, have a commitment to interoperable and secure technical standards, determined by internationally recognized standards bodies, as well as a commitment to protect intellectual property, including commercial trade secrets, from theft [9]. This element links to Sub condition 1.

While the CRI provides guidelines on how to assess the state of a nation's cyber security readiness, it remains a complex and daunting task. Defining a single metric to quantify the impact that people, software and systems have on cyber security is also highly improbable due to the number of factors involved in the process [3]. As a result of the mentioned uncertain nature and the varying fields affected by cyber security, a proliferation of adopted measurements has emerged (refer to **Error! Reference source not found.**). It is thus clear that some form of formalised structure is emerging in the information security community to standardise the way information security is measured and represented. This is a crucial step towards effectively measuring the security posture of an organisation and even on a larger scale a country.

3.2 Common Vulnerability and Exposures

One of the most frequently used metrics is the CVE metric as depicted in **Error! Reference source not found.Error! Reference source not found.**. CVEs are used to assess the security of software on a computer/device by disclosing specific vulnerabilities discovered in a structured format. While the metric is useful in describing a potential vulnerability that exists for a given software system, several shortcomings exist. While CVEs have a clearly defined structure making it useful to communicate to various individuals, the data entered into the respective fields are still very subjective and controlled by the creator of the specific CVE [1]. This opens up the potential for wrongful classification of a severity that could indicate that a device has a critical vulnerability when in fact the device is safe. This links to Sub condition 1.

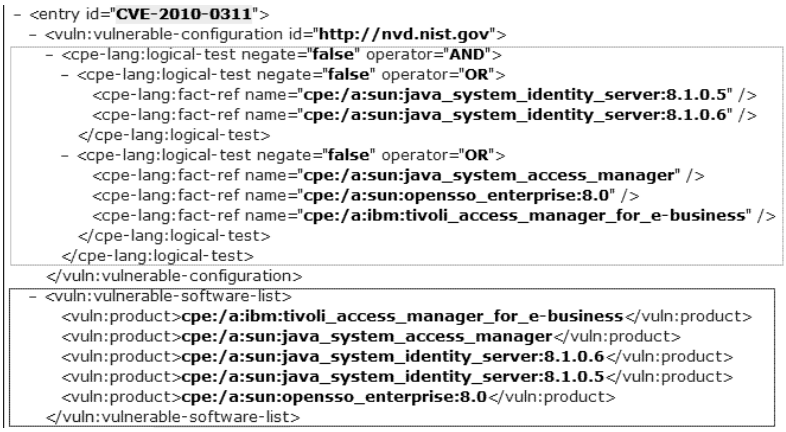

Fig. 2. CVE example

The uncertainty regarding the CVE critical score is but one of the problems with current measurements available. Several other factors such as the vulnerability recorded might simply be the by-product of an even bigger vulnerability that the researcher have missed. A further factor is that no single organisation controls the complete set of all available CVEs [5] and more importantly, the individual CVEs are contributed by the security community. This leads to duplication, differences in measurements and the possibility of software with severe vulnerabilities being completely missed. This links to Condition 1.

Even if all of the inconsistencies and inaccuracies are ignored and trust is placed in a reputable vendor, further technical challenges await. Work conducted by Espinahara and Eduardo [7] highlight just how inaccurate even the most sophisticated current information security assessment software can be. While the software works fine when the language is set to English, a simple change of system language can render the vulnerability scanner nearly useless. In essence this means that any measurement currently performed on non English computer systems has the potential to be grossly inaccurate. Furthermore, vulnerability scanners can mostly only identify vulnerabilities related to software while previously it was made clear that information security spans a whole range of categories that need to be taken into account.

While the use of CVEs proves to be useful in measuring some information security aspects, this method does not guarantee complete information security protection. There are many factors that can result in negative or skewed metric results. As a result, CVEs is not a fool proof method of measurement.

4 Mapping Traditional Warfare Metrics to Cyber Warfare

This section maps the traditional warfare factors identified in Section 1.3 to the cyber domain. This mapping is done in aid of developing a cyber military doctrine and establishing metrics to measure information security damage and potentially measure of loss due to cyber warfare. The aim is to prove the validity of the formula presented in Section 1.3 within the cyber domain. In proving this validity, each of the tradition-

al warfare conditions needs to be discussed in terms of the cyber (information security) domain. It should be noted that this mapping process is not straightforward since the Internet and cyber domain is largely intangible and therefore difficult to map to the real world traditional warfare domain.

4.1 Condition 1: Political Power Fluctuations

The offending nation state needs to have political power fluctuations present. For this condition to be true, the cyber actions should contribute to the nation state's political power fluctuations to some degree.

Especially since 2010's start of the Arab Spring, digital tools such as YouTube, Twitter and Facebook have defined many social movements by giving rise to a new generation of activism. In many of these uprisings, the Internet, mobile phones and social media played a pivotal role in the organising of protests by activists. Public information supplied by social networking websites has played an important role during modern-day activism, especially since it is employed as a key tool in expressing thoughts concerning unjust acts committed by the government [12]. In addition, *"digital media has been used by many protestors to exercise freedom of speech and as a space for civic engagement"* [18]. In this sense, freedom of speech can be classified as the political right to communicate one's opinions and ideas using one's body and property to anyone who is willing to receive them.

In addition, work done by Collier and Hoeffler, Collier et al. and Arnson (in [2]) have identified a link between civil wars and grievances such as inequality or a lack of political rights. It is believed that, although resources are central to the duration and intensity of war, the roots and objectives of war are often founded in politics. In the cyber domain, the high availability of Internet-based, low-cost cyber-weapons that can target civilian information assets has become a growing threat to the economic and political stability of modern societies that depend on today's information infrastructures [13]. In the cyber domain, political power fluctuations are extremely prevalent since the Internet is an artificial environment that can be shaped in part according to national security and political requirements. In addition, cyber attacks are flexible enough to be effective for information warfare and propaganda, espionage, and the destruction of critical infrastructure [20].

4.2 Condition 2: Potential for Lethality

For this condition to be true, the cyber actions should have the potential for lethality for at least one of the acts of cyber aggression. By extension of the definition for aggression (feelings of anger or antipathy resulting in hostile or violent behaviour, readiness to attack or confront), any act of cyber aggression can be regarded as having the potential for lethality. The acts of cyber aggression as identified by Carr [4], can be explained in the cyber domain as follows:

- **Cyber attacks against government or critical civilian websites or network without accompanying military force.** The recent breach of the South African Police's (SAPS) whistle-blowers' web portal is an example of a major cyber attack against a government. The dumped data contained numerous personally identifia-

ble records that could lead to the identification of people who have provided information to the SAPS in confidence.

- **Cyber attacks against government or critical civilian websites or network with accompanying military force**. Many high-profile cyber-attacks initially targeted the military. For example, the 1986 Cuckoo's Egg incident had Clifford Stoll tracking German hackers who were scouring American military systems. In 1994, hackers infiltrated Griffis Air Force Base computers to launch attacks at other military, civilian and government organisations [13].
- **Cyber attacks against internal political opponents**. If technology is utilised in internal political agendas, it is a real possibility that digital acts can result in physical violence. For example, the Tunisian part of Arab Spring saw Internet censorship, data harvesting by the government, laws restricting online freedom of expression and hactivism (as performed by Anonymous' *Operation Tunisia*). These online actions had a very tangible violent outset.
- **Cyber intrusions into critical infrastructure and networks**. Critical infrastructure protection is a crucial part of cyber protection, as was illustrated by the Stuxnet attack. If a nation state's national critical infrastructure is attacked, it can have a devastating impact on most aspects of civilians' lives, including transport, communication, water and sanitation, etc. For example, if the transport sector is affected, it would have an impact on all emergency services, since no fire brigade or ambulance would be able to perform their duties. If the communication sector is affected, it could potentially lead to large scale hysterics, since people will be unable to contact their friends and families. These scenarios have the potential for lethality.
- **Acts of cyber espionage.** Few nations can claim to not have been affected by some form of cyber espionage, either by participation or by victimisation [25]. Documents that were released by whistle-blower Edward Snowden have revealed just how prevalent cyber espionage is. These documents claim that the United States' PRISM program is capable of indiscriminately intercepting and analysing information received from email, phone and video. Similarly, the United Kingdom has admitted to spying on delegates for the G20 international summit in London 2009 [21]. In the APT1 report, the Mandiant group documents their search for a Chinese hacker group that has launched a massive espionage network affecting nations on all continents [15]. Figures from the report reveal that as much as four Terabytes of data has been exfiltrated from a single company; this is reckoned as the longest active backdoor found: four years and three months.

4.3 Condition 3: Needs of the Offending Nation State

For this condition to be true, either both the first two sub conditions, or the third sub condition needs to be true.

Sub Condition 1: False Optimism

The offending nation state needs to have false optimism regarding the outcome of the war. This condition is two-fold. Many cyber incidents receive little or no public

acknowledgment [13]. As such, people are often not informed about the actual extent and implications of cyber attacks. For example, at the time of writing, very little statistics are available for cyber crime in South Africa. This is largely due to the fact that no legislation is in place that obliges victims to report the crimes. There are a number of initiatives that allows for the reporting of crime in South Africa, but few of these cater for the reporting of cyber related crimes. As such, many crimes go unreported and the resultant available statistics are often skewed.

In addition, the enormous proliferation of technology and hacker tools makes it impossible to be familiar with all of the technology advances. Software updates and network reconfigurations also increase the unpredictability of the battlespace of cyber conflict with little or no warning [20]. As such, it becomes easy to have false confidence in one's cyber abilities, and accordingly, the outcome of a cyber war (refer to Section 3).

Sub Condition 2: Actions Lead to an Advantageous Position

The offending nation state needs to believe that their actions will lead to an advantageous position. Towards this end, the Internet has a number of salient characteristics that makes it a powerful tool in achieving this perceived advantage [6]. These are:

- **Reach.** The Internet has a global reach, with 2,405,518,376 Internet users in more than 233 countries worldwide [11]. This greatly enhances the potential for cumulative resources.
- **Ease.** Anyone with an Internet connection can become a cyber warrior or unwittingly allow their computer to be used as part of a zombie network.
- **Anonymity.** The Internet allows users to be completely anonymous, often giving people more confidence to say or do what they want online.

Sub Condition 3: Easy Conquest

In order for an offending nation state to believe that the war will be an easy conquest, the CRI can be used as measurement tool of cyber power on a governance level (refer to Section 3). Not only can the CRI be used to assess a nation state's own cyber capability to perform a cyber attack, but the target nation state's CRI can be assessed to predict the ease with which such a cyber attack will be performed and the technical skills with which the target will receive the attack and retaliate. In contrast with the process for traditional warfare, the proximity of adversaries is determined by connectivity and bandwidth, not terrestrial geography [20]

5 Testing the Formula for Predicting Cyber Warfare

In order to test the applicability of the formula for predicting warfare in the cyber domain, the validity of the conditions will be tested for the Israeli-Palestinian cyber conflict that took place between July 1999 and April 2002. A similar test was done to

test the formula on the Estonia cyber conflict. However, due to limited space, the rationale was not included in the article.

5.1 Condition 1: Political Power Fluctuations

In September 2000, Israeli teenage hackers created a website to jam Hezbollah and Hamas websites in Lebanon. The teenagers launched a sustained Distributed Denial of Service attack that effectively jammed six websites of the Hezbollah and Hamas organisations and the Palestinian National Authority. In response, Palestinian and other supporting Islamic organisations called for a cyber Holy War. Hackers struck three high-profile Israeli websites belonging to the Israeli Parliament, the Ministry of Foreign Affairs, and the Israeli Defence Force information site. They also targeted the Israeli Prime Minister's Office, the Bank of Israel and the Tel Aviv Stock Exchange [20]. By targeting political entities and by calling this war a cyber Holy War, the first condition of political power fluctuations can be considered as true, since there is a political undertone and a number of non-isolated acts occurred.

5.2 Condition 2: Potential for Lethality

As illustrated in Section 4.2, any attack on critical infrastructure has the potential for lethality. During the Israeli-Palestinian cyber conflict, attacks were made against companies providing telecommunications infrastructure [20]. Therefore, the condition of lethality potential can be considered as true.

5.3 Condition 3: Needs of the Offending Nation State

For this condition to be true, either both the first two sub conditions, or the third sub condition needs to be true.

Sub Condition 1: False Optimism

By January 2001, the Israeli-Palestinian cyber conflict had struck more than 160 Israeli and 35 Palestinian websites; 548 Israeli domain websites were defaced [20]. These conquests could potentially give both sides false optimism in terms of their chances of victory, rendering the first sub condition true.

Sub Condition 2: Actions Lead to an Advantageous Position

Palestinian hackers defaced an Internet Service Provider and left a message claiming that they could shut down the Israeli ISP NetVision, which hosts almost 70 percent of all the country's Internet traffic [20]. By disabling the opponent's Internet access, the Palestine side rendered the sub condition of performing actions to lead to an advantageous position true.

Sub Condition 3: Easy Conquest

In 2013, Israel's networked readiness index is ranked 15th up from rank 20 in 2012, whilst Palestine does not feature on the index. This year's index coverage includes a 144 economies, accounting for over 98 percent of global GDP. This presents an interesting point to consider that it could be possible for countries to not participate in such rankings and effectively allow potential aggressor nation states to believe that they are easy prey, whilst obfuscating their offensive cyber capabilities until it was too late.

5.4 Formula for Predicting Cyber Warfare

Based on the discussions above, the following conditions for predicting the possibility of cyber warfare are met:

Possibility of cyber warfare = Nation state political power fluctuations
AND Potential for lethality
AND ((False optimism
AND Offending nation state advantage)
OR Easy conquest)
= True
AND True
AND ((True
AND True)
OR True)

From this case study, it can be argued that the Israeli-Palestinian cyber conflict adheres to all the requirements to enable the early prediction of this cyber war.

6 Conclusion

Currently the only concrete way of measuring the status of the cyber domain is located in traditional information security techniques whether it be on a technical or policy level. While applicable, the measurements do not adequately describe loss, posture or any of the pre-requisites found in traditional warfare. Although it is possible to perform an analysis of characteristics of the ICT society with regard to domination threats, economic sustainability, etc., these measurements have not yet been employed according to the literature survey performed by the authors. Accordingly, this article aimed to provide evidence towards the probability of predicting and mapping traditional warfare measurements to the cyber warfare domain. As such, this article worked to find an alternative way of predicting the possibility of cyber warfare, since traditional information security measurements are not adequate.

The article looked at current information security metrics, the CRI and CVEs, and provided an alternative method of predicting the probability of cyber warfare. A formula predicting the possibility of traditional warfare was articulated based on existing literature. The conditions for this formula were mapped to cyber warfare theory to prove the validity of this formula in the cyber domain. In addition, this formula was

tested by applying it to the Israeli-Palestinian cyber conflict. This conflict is generally accepted as a cyber warfare incident. As such, the conditions are met by the acts of cyber aggression to affirm that cyber warfare took place. This article showed that the formula can be applied to the cyber domain. The value of this formula lies in the potential for pre-emptively identifying potential cyber war incidents. By pro-actively analysing global news and especially citizen journal journalism through social media platforms for indicators of the elements of the formula for predicting the possibility of cyber warfare, it may be possible to predict to occurrence of potential cyber war incidents, and as such, limit the potential damage caused, if the incidents cannot be prevented in totality. This extraction of collective intelligence falls beyond the scope of this article, but can be considered for future work in extending the formulate for predicting the possibility of cyber warfare.

References

1. Allodi, L. & Massacci, F. 2013. *How CVSS is DOSsing your patching policy and wasting your money*. Available from http://media.blackhat.com/us-13/US-13-Allodi-HOW-CVSS-is-DOSsing-Your-Patching-Policy-Slides.pdf (Accessed 20 November 2013).
2. Baten, J. & Mumme, C. 2013. Does inequality lead to civil wars? A global long-term study using anthropometrics indicators (1816-1999). *European Journal of Political Economy*. Volume 32. 56-79.
3. Boehme, R. and Freiling FC. 2008. *On metrics and measurements in Dependability metrics: Advanced lectures*. Eusgled, I., Freiling, FC. & Reussner, R. Eds. Springer, Heidelberg, Berlin, 7-13. DOI= http://dx.doi.org/10.1007/978-3-540-68947-8_2
4. Carr, J. 2011. *Inside Cyber Warfare.* O'Reilly Media: Sebastopol.
5. Christey, S. & Martin, B. 2013. *Buying into the bias: Why vulnerability statistics suck*. Available from http://attrition.org/security/conferences/2013-07-BlackHat-Vuln_Stats-draft_22-Published.pptx (Accessed 18 November 2013)
6. Delany, C. 2011. *Online Politics: The Tools and Tactics of Digital Political Advocacy.* Available from www.epolitics.com (Accessed 8 October 2013).
7. Espinahara, J. & Eduardo, L. 2013. *Lost in translation*. Available from: http://conference.hitb.org/hitbsecconf2013kul/materials/D2T3%20-%20Luiz%20Eduardo%20and%20 Joaquim%20Espinhara%20-%20Lost %20in%20Translation.pdf (Accessed 20 November 2013).
8. Filiol, E. 2011. Operational aspects of cyberwarfare or cyberterrorist attacks: What a truly devastating attack could do. In: *Leading issues in information warfare & security research.* Ed: Ryan, J. Academic Publishing: Reading. Volume 1. 35-53.
9. Hathaway, M. 2013. *Cyber readiness index 1.0.* Available from: http://belfercenter.hks.harvard.edu/files/cri-methodology-1-point-0-final.pdf (Accessed 21 November 2013).
10. Heickerö, R. 2007. *Some aspects on cyber war faring in information arena and cognitive domain.* Available from: http://www.dodccrp.org/events/11th_ICCRTS/html/ presentations/157.pdf (Accessed 25 November 2013).
11. Internet World Stats. 2013. *Internet usage statistics - The internet big picture.* Available from: http://www.internetworldstats.com/stats.htm (Accessed 29 October 2013).
12. Kassim, S. 2012. *Twitter revolution: How the Arab Spring was helped by social media.* Available from: http://www.policymic.com/articles/10642/twitter-revolution-how-the-arab-spring-was-helped-by-social-media (Accessed 9 October 2013).

13. Knapp, KJ. & Boulton, WR. 2006. Cyber-Warfare Threatens Corporations: Expansion into Commercial Environments. *Information Systems Management*. Volume 23(2). 76-87.
14. Liles, S., Rogers, M., Dietz, JR. & Larson, D. 2012. *Applying traditional military principles to cyber warfare.* Available from: http://www.ccdcoe.org/publications/ 2012proceedings/3_2_Liles&Dietz&Rogers&Larson_Applying TraditionalMilitaryPrinciplesToCyberWarfare.pdf (Accessed 25 November 2013).
15. Mandiant. 2013. Exposing One of China's Cyber Espionage Units. Available http://intelreport.mandiant.com/ Mandiant_APT1_Report.pdf (Accessed 19 November 2013).
16. MITRE. 2012. *By Cyber Security Area.* Available from: http://measurablesecurity. mitre.org/directory/areas/ index.html (Accessed 29 November 2013).
17. Oxford Dictionaries. 2013. Cyberwar. Available from: http://www.oxford dictionaries.com/definition/english/ cyberwar (Accessed 22 November 2013).
18. PewResearch, 2012. *The role of social media in the Arab uprisings.* Available from: http://www.journalism.org/ 2012/11/28/role-social-media-arab-uprisings/ (Accessed 9 October 2013).
19. Rid, T. 2012. Cyber war will not take place. *Journal of Strategic Studies.* Volume 35(1), 5-32.
20. Schreier, F. ND. *On cyberwarfare.* DCAF Horizon 2015 Working Paper No. 7.
21. Symantec. 2013. *Internet Security Threat Report (ISTR).* Volume 18. Available from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_ v18_2012_21291018.en-us.pdf (Accessed 30 November 2013).
22. UNICRI. ND. *Cyberwarfare.* Available from: http://www.unicri.it/special_topics/ cyber_threats/cyber_crime/ explanations/cyberwarfare/ (Accessed 22 November 2013).
23. Van Evera, S. 1999. *Causes of war: Power and the roots of conflict.* Cornell University Press: New York.
24. Van Niekerk, B. & Maharaj, MS. 2011. *The Information Warfare Life Cycle Model.* SA Journal of Information Management 13(1), Art. 476.
25. Verizon. 2013. *The 2013 Data Breach Investigations Report.* Available from: http://www.verizonenterprise.com/ resources/reports/rp_data-breach-investigations-report-2013_en_xg.pdf (Accessed 18 November 2013).