COMPUTERS & SECURITY 49 (2015) 70–94

Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/cose

Computers & Security

Cyber warfare: Issues and challenges

Michael Robinson [a,*], Kevin Jones [b], Helge Janicke [a]

[a] Faculty of Technology, De Montfort University, Leicester, United Kingdom
[b] Cyber Operations Team, Airbus Group Innovations, Newport, United Kingdom

ARTICLE INFO

Article history:
Received 29 July 2014
Received in revised form
13 November 2014
Accepted 18 November 2014
Available online 29 November 2014

Keywords:
Cyber war
Cyber warfare
Information Warfare
Cyber Security
Cyber Conflict

ABSTRACT

The topic of cyber warfare is a vast one, with numerous sub topics receiving attention from the research community. We first examine the most basic question of what cyber warfare is, comparing existing definitions to find common ground or disagreements. We discover that there is no widely adopted definition and that the terms cyber war and cyber warfare are not well enough differentiated. To address these issues, we present a definition model to help define both cyber warfare and cyber war. The paper then identifies nine research challenges in cyber warfare and analyses contemporary work carried out in each. We conclude by making suggestions on how the field may best be progressed by future efforts.

1. Introduction

Throughout history, mankind has waged war, seeking to further national agendas in an ever changing international game of power. From the sword battles of the past to the unmanned drone strikes of today, this game of power is constantly driven to shift and evolve by technology. The development of armoured vehicles, aircraft, ships and the use of electronics and telecommunications have all expanded the battle space and introduced new and innovative ways to gain an advantage over opponents. Just as the technological innovation of flight triggered a race to dominate the skies, the emergence of cyberspace has opened up new strategic possibilities and threats, causing a scramble to secure a dominant position inside of it (Apps, 2012).

Increasing media coverage of cyber warfare (Watts, 2011; Marcus, 2013; Krever, 2013) has only served to heighten public awareness that cyberspace is becoming an arena of warfare. Governments, too, are fully aware of the need to take action in response to threats from cyberspace. US President Barack Obama has declared America's digital infrastructure a strategic national asset, and formed Cybercom: a division inside the Pentagon whose stated task is to "perform full spectrum operations" (War in the fifth domain, 2010). Documents leaked from the National Security Agency in the US also confirm that national security figures are seeking to establish offensive cyber capability (Schneier, 2013). In the UK, government officials have warned of a lack of preparedness for cyber warfare and have announced new investments to bolster defence, such as the National Cyber Security Programme (Uk 'complacent' over military cyber-attack risk, mps warn, 2013). NATO has also been raising awareness, releasing the Tallinn Manual on the International Law Applicable to Cyber Warfare (NATO, 2013) as an attempt to advise nations on how to operate legally in this new war fighting domain. Looking at this evidence, it is clear that cyber warfare is a topic of global concern.

* Corresponding author.
E-mail address: michael.robinson@eads.com (M. Robinson).
http://dx.doi.org/10.1016/j.cose.2014.11.007

Conflict and war in any form has the potential to touch every person, whether as a combatant, relative of a combatant, civilian, business entity or nation state. This makes research into cyber warfare both valuable and essential to solve the growing number of issues raised by this new domain of war. Contemporary research into the topic is wide ranging, covering a number of sub topics ranging from legal issues on lawful combatancy to attempts to precisely define what a cyber weapon is. For anyone attempting to approach the field of cyber warfare, there is a challenge in gathering an understanding of all issues involved, how they relate to each other, what the current state of research is and where future research is required.

We address this problem, by providing an analytical survey of the current state of research into the area of cyber warfare. An analysis of the varying views and research carried out to date provides a discussion from which significant research areas can be identified and new research questions formulated.

Section 2 of this paper presents and analyses the various definitions of cyber war and warfare offered by the research community. Section 3 presents our definition model, and demonstrates how it can be used to reach definitions of not just cyber warfare, but any cyber situation. Section 4 then moves on to identify research challenges in cyber warfare, providing analysis of the views in each area. We then reach our conclusions and provide discussion on the direction future research should take.

1.1. *Methodology*

The identification of literature for analysis in this paper was based on a keyword search. These keywords were initially "Cyber War" and "Cyber Warfare". As subtopics such as cyber weapons and cyber deterrence were discovered, these also became keywords for further searches. Searching for these keywords in academic databases (Jesson and Lacey, 2011) such as IEEExplore and the ACM Digital Library, an initial set of relevant sources were located. Keeping in mind that cyber warfare is an interdisciplinary subject, journals from other disciplines such as law, international relations and defence were also searched for relevant sources. The keywords were also entered into common internet search engines such as Google, allowing the discovery of articles not indexed in digital libraries. To locate any sources that our keyword searches missed, a snowballing methodology was used (Wohlin and Prikladnicki, 2013). This methodology allowed the building of a reasonably complete picture of the current research landscape, and the identification of seminal works in the area by looking at citation frequencies. Although a systematic collection of literature has been performed, research (Kitchenham et al., 2011) has shown that relevant primary sources can be missed during searches, and that multiple researchers working to the same methodology will collect differing bodies of articles. Whilst this variation in literature searching cannot be avoided, the effects of it can be mitigated by providing this description of how the search process was performed.

1.1.1. *Inclusion criteria*

The search process produced a significant number of results. To ensure that only relevant sources were included for review, articles discovered by the search process were measured against a number of criteria. Each source had to meet one or more of the following requirements:

- The source directly addresses at least one specific aspect of cyber war or cyber warfare, such as ethics or deterrence.
- The source is not directly related to cyber war or cyber warfare, but provides a definition of one or both.

The use of such criteria resulted in certain material including works on the art and science of military conflict (Lonsdale, 2004; Tzu, 2005; Paret, 1986) not being included. Although arguably relevant in helping to understand the wider debates of conflict and war, such works have been excluded to achieve the paper's aim of providing a concise introduction to the immediate challenges and issues facing research into cyber warfare.

1.1.2. *Ranking of sources*

Each collected source was evaluated against five criteria and scored against it on a scale of one to three, with three being the best. The higher the overall score, the higher the source was ranked on our list. Using this ranking system allowed the prioritisation of sources. The criteria were as follows:

- Reputation – A source from a well respected organisation or author scores higher than one from a lesser known entity.
- Relevance – A measure of how the contents of the source relate to the topic at hand.
- Originality – Sources that offer new arguments, raise new issues or attempt to provide innovative solutions scored higher.
- Date of publication – More recently published sources were given a higher score than older ones.
- References – Sources which build upon, analyse or acknowledge previous work score highly.

2. Finding clear definitions

The first logical step in removing confusion from the area of cyber warfare is to define the various terms used in literature. The paper will therefore begin by analysing existing definitions offered by the research community. We consider four relevant terms that need to be distinguished in this field: Information Warfare, Cyberspace, Cyber Warfare and Cyber War. Often used interchangeably, these terms lack clear and agreed upon definitions and are a good starting point to better define the issue at hand.

2.1. *Cyberspace*

The most basic question to ask when examining cyber warfare is: What is cyberspace? Daniel Kuehl (2009) has examined this question. Kuehl collected and analysed the various definitions offered by a selection of sources including academic authors, U.S. Department of Defense documents and even science fiction. His analysis of existing definitions led him to conclude that cyberspace is more than just computers and digital

information, and that there are four aspects of cyberspace that a definition should reflect:

- An operational space – People and organisations use cyberspace to act and create effects, either solely in cyberspace or across into other domains.
- A natural domain – Cyberspace is a natural domain, made up of electromagnetic activity and entered using electronic technology.
- Information based – People enter cyberspace to create, store, modify, exchange and exploit information.
- Interconnected networks – The existence of connections allowing electromagnetic activity to carry information.

To reflect these four aspects, Kuehl offers his own definition of cyberspace:

> "A global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies." (Kuehl, 2009)

The definition offered by Kuehl is a comprehensive one that accurately communicates the unique aspects of cyberspace. It is therefore the definition of cyberspace that this paper adopts.

2.2. *Information warfare*

The term "information warfare" has a long history. The earliest recorded use of the term was by Thomas Rhona in 1976. Rhona defined information warfare as:

> "The strategic, operation, and tactical level competitions across the spectrum of peace, crisis, crisis escalation, conflict, war, war termination, and reconstitution/restoration, waged between competitors, adversaries or enemies using information means to achieve their objectives." (Libicki, 1995)

Martin Libicki argued that Rhona's definition was too broad, and stated that trying to define information warfare was like "the effort of the blind men to discover the nature of the elephant: the one who touched its leg called it a tree, another who touched its tail called it a rope, and so on" (Libicki, 1995). Rather than give a definition of information warfare, Libicki suggested that the term must be broken down into smaller parts to become understandable and meaningful. He therefore described seven forms of information warfare, shown in Table 1.

As can be seen by Libicki's thoughts on information warfare, the term is extremely broad. It can include denying battlefield commanders information, keeping sensitive messages secret, spreading propaganda, traditional hacking and so on.

Dorothy Denning provides an alternative definition of information warfare, stating that it "consists of offensive and defensive operations against information resources of a win-

Table 1 – Libicki's seven forms of information warfare (Libicki, August 1995).

Form	Description
Command-and-control	Attacks on command centres, or commanders themselves to disrupt command effectiveness
Intelligence-based	Increasing your own situational awareness while reducing your opponent's
Electronic	Use of cryptography and degrading the physical basis for transferring information (e.g. radar jamming)
Psychological	Use of information against the human mind. Propaganda to demoralise troops or influence civilian populations
Hacker	Exploitation of viruses, logic bombs and trojan horses to attack computer systems
Economic information	Possessing and being in control of information leads to power
Cyber	Information terrorism, semantic attack, simula-warfare, Gibson-warfare

lose nature (Denning, 1999). From Denning's perspective information warfare can be seen as a game, played between defenders and attackers who are in direct competition. Defenders perform defensive operations to protect information in any form, seeking to maintain its confidentiality, integrity and availability. Attackers perform offensive operations, seeking to damage that confidentiality, integrity and availability. Denning (1999) argues that information warfare can occur in a number of domains such as crime, individual rights and national security. Similar to Libicki (1995), the description of information warfare offered by Denning is broad. Kopp (2000) states that the aim of information warfare is to: "corrupt, deny, degrade and exploit adversary information and information systems and processes while protecting the confidentiality, integrity and availability of one's own information".

Taking these definitions of information warfare, it is clear that the term can be used to describe a very wide range of activities that include but also go beyond cyber space. The question of whether cyber warfare is simply a form of information warfare is unclear. To provide a better understanding of how cyber warfare relates to information warfare, we examine and analyse definitions of cyber warfare offered by the research community.

2.3. *Cyber warfare*

The term cyber warfare is one that is used in mainstream media and as with information warfare, there are many differing definitions. In 2001, Alford (2001) defined cyber warfare as:

> "Any act intended to compel an opponent to fulfill our national will, executed against the software controlling processes within an opponents system."

This definition from Alford reflects the view that cyber warfare is something that states will engage in to advance a national agenda. It can be argued, however, that modern warfare does not always aim to advance such an agenda. Religious beliefs and ideologies that are not tied to a national agenda can arguably be the aim of modern warfare. It therefore seems unwise to confine a definition of cyber warfare to having the purpose of advancing a national will.

Jeffrey Carr (2012) offers another definition of cyber warfare:

> "Cyber warfare is the art and science of fighting without fighting; of defeating an opponent without spilling their blood."

In comparison to Alford's (2001), this definition avoids attempting to define the motivation of the fighting parties. However, the suggestion that cyber warfare will not spill blood must be questioned. A cyber attack on critical national infrastructure, such as the power grid may result in loss of life. Colarik and Janczewski (2011) agree with this point, arguing that cyber warfare cannot be seen as bloodless.

Parks and Duggan (2011) offer another definition:

> "Cyberwarfare is a combination of computer network attack and defense and special technical operations."

This is a very broad definition of cyber warfare, which avoids the issue of who is taking part and why. Due to this it is difficult to fault their definition, other than it being potentially too broad. With regards to "special technical operations" (Parks and Duggan, 2011), Parks and Duggan refer to a US Department of Defense document which describes what these operations involve.

Arquilla and Ronfeldt (1993) do not define cyber warfare, but instead offer a definition of cyberwar:

> "Cyberwar refers to conducting, and preparing to conduct, military operations according to information-related principles. It means disrupting if not destroying the information and communications systems, broadly defined to include even military culture, on which an adversary relies in order to know itself: who it is, where it is, what it can do when, why it is fighting, which threats to counter first, etc. It means trying to know all about an adversary while keeping it from knowing much about oneself. It means turning the balance of information and knowledge in ones favor, especially if the balance of forces is not. It means using knowledge so that less capital and labor may have to be expended"

Arquilla and Ronfeldt see cyberwar as a battle for control over information and communication flows, with the ultimate aim developing an advantage over an opponent. In this respect, there are similarities with the ideas of information warfare. The definition does however face the same challenge as Carr's (2012), in that attacks intended to cause physical damage are not accounted for.

Another definition of cyber warfare is put forward by Cornish et al. (2012):

> "Cyber warfare can be a conflict between states, but it could also involve non-state actors in various ways. In cyber warfare it is extremely difficult to direct precise and proportionate force; the target could be military, industrial or civilian or it could be a server room that hosts a wide variety of clients, with only one among them the intended target."

This definition raises the idea that non-state actors may be involved in cyber warfare, an interesting idea that other definitions miss. The use of "can be", "could" and "various ways" make it a general definition that would benefit from being more distinct. It also highlights that cyber warfare may be unpredictable and imprecise in its effects – an idea that is missing from other definitions.

Taddeo (2012) defines cyber warfare as:

> "The warfare grounded on certain uses of ICTs within an offensive or defensive military strategy endorsed by a state and aiming at the immediate disruption or control of the enemys resources, and which is waged within the informational environment, with agents and targets ranging both on the physical and non-physical domains and whose level of violence may vary upon circumstances"

This definition gives a motivation: the immediate disruption or control of enemy resources. The "immediate" aspect may be challenged, however, since certain attacks may have a delayed effect, rather than an immediate one. The suggestion that targets may be physical and non-physical is an interesting point missing from other definitions, and represents cyber warfare having the potential to inflict kinetic effects.

Agreeing with Taddeo's (2012) school of thought, Billo (2004) defines cyber warfare as:

> "Units organized along nation-state boundaries, in offensive and defensive operations, using computers to attack other computers or networks through electronic means."

Here Billo is suggesting that attackers are organised along nation state boundaries. This appears to be a very traditional view of warfare in the cyber domain. It is unclear on how Billo sees nation state boundaries. If they are seen as the physical borders of a nation, then this is a weakness since combatants in cyber warfare may be highly geographically dispersed across multiple nations. If he means on cyber boundaries (i.e. at tier one internet backbones) then this becomes more reasonable, but still places a locational limitation on cyber warfare that may not exist.

Richard A. Clarke, special advisor on cyber security to US president Bush (2001–2003), defines cyber war as:

> "Actions by a nation state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke and Knake, 2010).

Similar to the definitions provided by Taddeo (2012) and Billo (2004), this is a very nation state focussed definition.

The Oxford English Dictionary contains its own definition of cyber warfare, stating that it is simply "another term for

cyber war". The definition given for cyber war is: "The use of computer technology to disrupt the activities of a state or organization, especially the deliberate attacking of communication systems by another state or organization" (Oxford English Dictionary, 2013). As with the other definitions examined, it can be argued that this definition is problematic. Firstly, it is unclear why the emphasis on communications systems is necessary. Many systems can be at risk from cyber warfare, including critical national infrastructure such as the power grid and transportation networks (Nicholson et al., 2012). Secondly, the assertion that cyber war and cyber warfare are synonymous can be challenged, since the dictionary itself provides contradicting evidence. Rather than defining the well understood and established term of warfare as another term for war, it defines it as "Engagement in or the activities involved in war or conflict" (Oxford English Dictionary, 2013). This raises an important question: If war and warfare have separate definitions that appear to make sense, why has the Oxford Dictionary chosen to state that cyber warfare is simply another word for cyber war?

2.4. *Summary of existing cyber warfare definitions*

An examination of the literature has demonstrated that there is no widely accepted definition of cyber warfare. Some researchers offer very broad definitions, which do tend to cover most imaginable cases of cyber warfare but are potentially too broad. Others give very specific definitions, which are potentially more useful but then fail to cover certain elements of what could be considered cyber warfare. Definitions from other sources such as the Oxford English Dictionary have also been shown to be problematic. With usage of the term increasing in political and media circles (Vlahos, 2014; Wilking, 2013), the lack of a methodically reached definition is a problem that needs to be addressed. To resolve this problem, we propose a definition model that is based upon the identification of actors and intent.

3. The Actor and Intent Definition Model

The Actor and Intent Definition Model provides a methodical process from which definitions of harmful events in cyber space can be reached. It is based upon the idea that all hostile cyber situations can be broken down into two basic concepts: An actor launching a cyber attack, with some kind of harmful intent. To use these two concepts, it is first important to be clear on their meanings.

3.1. *Cyber attack*

In our model, a cyber attack is the basic building block that is common to all hostile cyber situations. We define a cyber attack as follows:

Definition 1. Cyber Attack. An act in cyber space that could reasonably be expected to cause harm.

Harm is defined in its broadest sense: economic, psychological, physical, reputational, strategic and so on.

3.2. *Intent*

Once it has been established that an actor has launched a cyber attack, it is necessary to determine the intent behind that attack. The fundamental question to be asked here is: What was the purpose of the harm? Presented here are some examples of non-cyber situations, along with the commonly associated intent:

Situation	Common intent
Warfare	Achieving military objectives
Crime	Personal gain through illegal means.
Bullying	Causing psychological distress to another individual.
Espionage	Obtaining political or military information covertly.
Terrorism	Influence a nation's policies through violence and fear.

3.3. *Actor*

The entity that carried out the cyber attack must also be considered alongside the intent. Consideration of the actor improves the chances of coming to a correct conclusion on their intent. If the actor is a state, a conclusion of warfare-like intent would arguably be easier to reach than if the actor was an individual. If the actor is a known terrorist group, conclusions of terrorism-like intent are arguably more feasible. This cannot be a formulaic process however: it cannot be said that an individual can never have warfare-like intents, or that a terrorist group automatically has terrorism-like intents. Therefore, it is a human process of weighing up actor and intent to reach a subjective conclusion on how the cyber event should be defined.

3.4. *Reaching a definition of a cyber event*

Having considered the actor and the intent, we can define a cyber situation by comparing it to a non-cyber situation. For example, if a cyber attack was launched by a nation state with the intent of achieving a military objective, this cyber situation is defined as cyber warfare. If an individual launched a cyber attack with the intent of causing psychological distress to another individual, it can be concluded that cyber bullying has taken place. By following this method, we can define almost any cyber situation, including cyber warfare.

3.5. *Reaching a definition of cyber warfare*

By applying the actor and intent definition model, we reach the following definition for cyber warfare:

Definition 2. Cyber Warfare. The use of cyber attacks with a warfare-like intent.

3.6. Reaching a definition of cyber war

The reviewed literature also made reference to cyber war, with some sources stating that it was a synonym with cyber warfare. It can be argued that this is not the case. As stated, cyber warfare is an activity – the use of cyber attacks with a warfare-like intent. Cyber war on the other hand is a state of being. An actor can be at war, but does not perform war – they perform warfare. We therefore present a definition of cyber war:

> **Definition 3.** Cyber War. Occurs when a nation state declares war, and where only cyber warfare is used to fight that war.

The key to a situation being classed as a cyber war is that cyber warfare is the only type of warfare used. If a kinetic attack is used during the war, such as an air strike, the situation should not be classified as cyber war – it should simply be seen as war where cyber warfare was used.

3.7. Example scenarios

To test these definitions of cyber war and cyber warfare, it is useful to present a number of potential scenarios and see how they evaluate:

3.7.1. Country A vs country B

Country A openly declares war against country B, and uses its military to conduct coordinated cyber attacks. These attacks are aimed at country B's power grid, and are successful in causing disruption to the power supply. Power plants go down and blackouts occur, leaving much of the nation without power. Country A takes advantage of the blackout in country B to launch an air strike, bombing an air base whilst situational awareness is impaired.

Examining the actor and intent, this scenario involves a nation state launching a cyber attack with the intent of achieving a military objective. This matches a warfare-like intent and the situation can initially be described as cyber warfare. With the addition of a declaration of war, however, the situation is upgraded to cyber war. Once the air strike is carried out, a kinetic attack has been used. This transforms the situation. Since cyber warfare is no longer the only type of warfare being used, the situation cannot be called cyber war. The situation is now best defined simply as war – one that uses both kinetic and cyber warfare.

3.7.2. Country C vs country D

Country C detects a number of cyber attacks coming from country D. These attacks intend to steal information from a large electronics manufacturer based in country C and from country C's commerce and trade ministry. There is no proof that these attacks are state sponsored, but coding in some analysed malware suggests country D might be responsible. The attacks remain ongoing for many years, but country C focuses on strengthening its cyber defences rather than overtly confronting country D.

Many grey areas exist in this scenario, but the intent model can help to define it by looking at the intent of the attacks. In this case, the attacks are aimed at accessing information from industry and from the commerce and trade ministry. The intent behind such attacks can be narrowed down to a handful of possibilities. Financial gain is a possibility – the actor may wish to sell trade secrets on the black market, or use them in their own business. These are crime-like intents, suggesting that cyber crime is a potential candidate for this scenario. Economic intent by a nation state is also a possibility. With access to confidential information from the trade ministry, and details of production at a large electronics firm, a nation may be able to achieve an advantage in international trade and commerce. This is an espionage-like intent, and makes cyber espionage also a possible label for this situation. We can at the very minimum state that this situation is a cyber attack – an act has occurred in cyber space that could reasonably be expected to cause harm. As more evidence on the intent and perpetrator emerge, the model can more firmly begin to categorise the attack. This is a strength of the model, since the way it defines a situation can evolve and become more certain as additional information on the event becomes available.

3.8. Advantages of the definition model

Fig. 1 gives a visual representation of our definition model, and shows the process of how definitions of cyber events can be reached. The model has a number of advantages. Firstly, the model reflects the fact that international events can not always be defined straightforwardly. An uprising in a state may be labelled as terrorism by the state but as revolution by others. In February of 2014 Russia announced its concern that the Ukraine had been taken over by terrorists (Traynor, 2014). Months later in April, it is the Ukraine government claiming to be conducting anti-terror operations, to remove pro-Russian forces from the country (Ukraine says donetsk 'anti-terror operation' under way, 2014). Clearly terms such as terrorism have a subjective element that a strictly systematic methodology could not capture. Our model allows for this human element by requiring the concept of intent to be considered. A second advantage of our model is that it removes the need to invent a new definition for every new cyber situation. Our model shows that this is unnecessary, since we can simply take the existing definition of a kinetic situation, and use it to define the cyber equivalent. For completeness, the following gives some examples of this advantage.

3.9. Applying the model to cyber terrorism

The FBI define terrorism as: "Violent acts or acts dangerous to human life that violate federal or state law and appear to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping" (FBI, 2014).

Taking this definition, we can define cyber terrorism by identifying who is launching the cyber attack and the harmful intent behind it. The FBI definition does not state a particular group, so it can be assumed that the who is any person or organisation. Cyber terrorism can therefore be defined as:

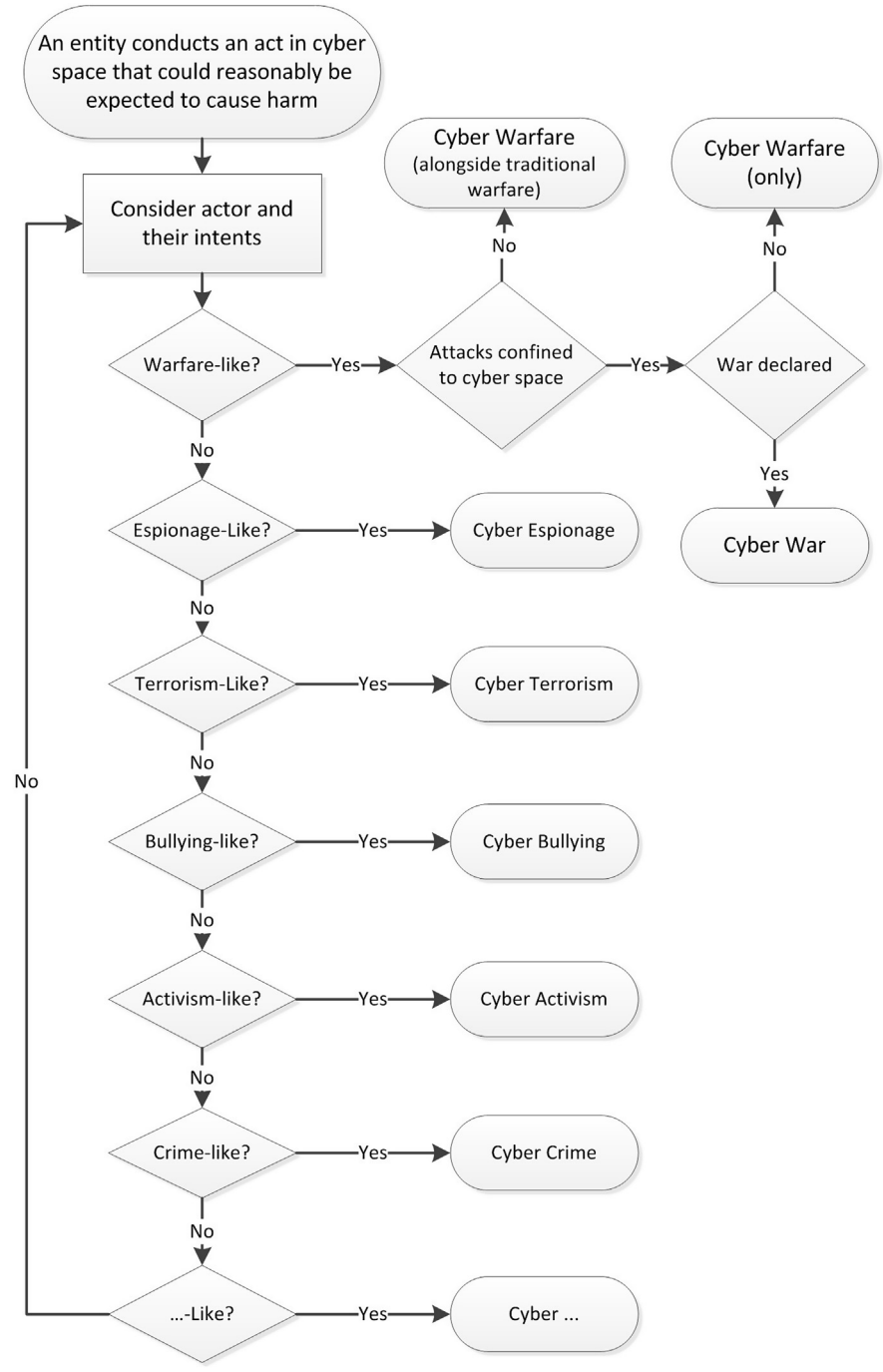

Fig. 1 – Actor and intent definition model.

> "Cyber attacks where the intent is to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination or kidnapping."

Using this definition, a cyber attack on a nuclear power plant with the intent of causing mass destruction would be cyber terrorism. While assassination via cyber means may sound extreme, it is possible to envisage an air defence system being compromised by cyber means to target an aircraft it ordinarily would not. Cyber kidnap may become an issue if fully automated vehicles become commonplace. Quite simply, it would be nothing more than a cyber attack with kidnapping-like intents. Whether the international community wishes to differentiate between terrorism and cyber terrorism is another matter that is beyond the scope of this paper. They may see terrorism as terrorism, with the method of delivery as

insignificant. This paper simply uses cyber terrorism here as evidence that our model can be used to define it.

3.10. *Applying the model to cyber crime*

Crime can have many intents in the kinetic world including financial gain, revenge, or a hatred of another person. These intents do not change simply because the delivery is via cyber attack, and therefore no new definitions are required. If a cyber attack occurs, and the intent behind it matches a criminal intent, then cyber crime has occurred.

3.11. *Summary of the Actor and Intent Model*

In this section our actor and intent definition model was presented, which addressed the previously identified problem of trying to define cyber warfare. The model asserts that it is possible to reach a definition of any cyber situation by examining who is doing a cyber attack and why. This was demonstrated by reaching definitions of cyber warfare and cyber war. A number of scenarios were presented, to demonstrate how the model could be extended to define other cyber situations such as cyber terrorism.

4. Research challenges in cyber warfare

With both cyber warfare and cyber war better defined, it is prudent to examine the current state of research in the area. This section identifies nine topics that have presented challenges to the cyber warfare research community. These are shown in Fig. 2.

4.1. *Early warning systems*

Early warning (EW) systems have long been a significant area in military intelligence and provide the ability to detect when an adversary is undertaking preparations to launch an attack and what that attack may consist of. In traditional kinetic warfare, EW systems are well established. Intelligence officers study satellite imagery and listen to communications, looking for known indicators of military mobilisation. In the cyber domain, however, it is unclear what these indicators are or how they can be observed. This presents a problem when trying to develop early warning systems for cyber warfare.

Fig. 2 – : Research challenges in Cyber warfare.

The first challenge in this area is to determine what a cyber early warning system should aim to achieve. Golling and Stelte (2011) address this question, by claiming that an EW system must provide answers to the following:

- Is a cyber war taking place right now/about to begin?
- Who is attacking?
- What is the target?
- What kind of attack methods are being used?

Looking at these questions, it can be argued that cyber warfare early warning has much the same goals as traditional early warning systems. But the problem of what to look for to answer these questions still remains. The field of cyber security has a tremendous amount of ongoing research into the area of attack detection, but as the name suggests it is focussed on detecting attacks as they happen, rather than providing an early warning of an impending attack.

Sharma et al. (2010) have argued that a cyber early warning system must consider more than just technical indicators. They state that many cyber attacks are associated with social, political, economic and cultural conflicts, and that to predict incoming cyber attacks these aspects must be considered. Moran (Carr, 2012) agrees with this view and has suggested that there are four stages that occur before a politically motivated cyber attack, which can be used as indicators for a cyber early warning system. These are shown in Fig. 3.

Moran's five stage model (Carr, 2012) combines political awareness with technical awareness to form an early warning system. It does however have some weaknesses. Firstly, Moran admits that the first two steps, latent tensions and cyber recon are not always necessary stages for a politically motivated cyber attack. If the first two steps in Fig. 3 are removed, we are left with just a three stage model: an initiating event, cyber mobilization and cyber attack. However, Moran (Carr, 2012) asserts that the most dangerous and sophisticated politically motivated attacks will follow the full five stages, and that only unsophisticated politically motivated attacks will follow the shortened, three stage model. Secondly, the order of the stages should be challenged. Moran's model (Carr, 2012) asserts that tensions lead to recon, and that some initiating event then triggers a cyber mobilisation, whereby "patriotic hackers are incited into action" (Carr, 2012). According to the model, these patriotic hackers then carry out the cyber attacks. It must be argued that this surely cannot always be the timeline of events in a politically motivated attack. It is possible to imagine a scenario whereby latent tensions exist but no recon takes place until after the initiating event. This results in a four stage model, with cyber recon placed after the initiating event. The usefulness of having stages presented in a fixed chronology is therefore

Fig. 3 – : Moran's five stages of politically motivated cyber attack (Carr, 2012).

brought into question. Despite these problems, Moran has presented some useful indicators that can be used in future early warning system research.

Fuller (2003) puts forth the argument that caution must be used when designing early warning systems in the cyber domain. He describes how in 1998, the U.S. introduced The Federal Intrusion Detection Network (FIDN) – a program to centrally monitor internet traffic passing through critical infrastructure, looking for anomalies in traffic that may alert to an impending attack. The network was dismantled after its existence became publicly known, leading to objections from civil liberties groups and privacy advocates. Clearly there is a need to balance granularity of monitoring with public expectations of privacy, and this is a point that should remain in the minds of those designing future EW systems for the cyber domain.

The challenge of creating a cyber warfare EW system has a significant amount of overlap with other research areas. Cyber security topics such as situational awareness, attack prediction, intrusion detection and network monitoring are all active research areas that will have an impact on the future of cyber warfare EW systems. But as Moran (Carr, 2012) and Sharma et al. (2010) state, cyber early warning cannot be approached from a purely technical perspective. An effective early warning system for the cyber domain will require an awareness of and significant input from other disciplines such as international relations and sociology.

4.2. *Ethics of cyber warfare*

As with any activity that has the potential to cause harm, cyber warfare presents ethical challenges. In particular, nations need to know when it is ethically justified to resort to cyber warfare and how to conduct such warfare ethically. Taddeo (2012) explains that traditional wars are guided by Just War Theory (JWT) (Taddeo, 2012) – a number of well defined principles stating when a nation is ethically justified to go to war, and how to remain ethical during one. Taddeo argues that these principles are difficult to apply when it comes to cyber warfare, and that these difficulties are worthy of further research.

In particular the principle of last resort is contentious. The spirit of this principle is that a bloody, harmful war should be avoided until all other avenues have been exhausted. Taddeo argues that this principle does not apply to cyber warfare, and that resorting to it early may be considered the ethical decision. The reasoning behind this view is that a cyber war would have little or no bloodshed. If this is the case, resorting to cyber war early would be ethically justified, since if differences can be resolved in this bloodless manner, the need for a more violent kinetic war can be avoided.

This view has a counter argument, however, in that cyber warfare should not automatically be considered less bloody than a kinetic war. Kinetic warfare can target specific military targets, and is guided by well established rules such as the laws of armed conflict and the Geneva Protocols. Cyber warfare on the other hand is currently much less regulated and decoupling military targets from civilian ones can be more problematic. Cyber attacks on national infrastructure could leave civilians without essential services such as power and food supplies, causing indiscriminate suffering in civilian populations. It may also cause physical harm in the form of explosions at power plants, failings at water treatment plants or interruptions to air traffic control systems. With this in mind, caution must be used before stating that it is ethical to resort to cyber warfare early.

Taddeo attempts to address the challenge of cyber warfare ethics by putting forward three principles that form a "Just Cyber War". These principles relate to an idea of an "infosphere". Taddeo defines this as "the environment in which animate and inanimate, digital and analogue informational objects are morally evaluated".

1. Cyber war ought to be waged only against those entities that endanger or disrupt the wellbeing of the Infosphere.
2. Cyber war ought to be waged to preserve the well-being of the Infosphere.
3. Cyber war ought not to be waged to promote the well-being of the Infosphere.

Point 1 represents the notion that cyber war is justified to eliminate negative influences on the well-being of the Infosphere. The next two points reflect the view that cyber war should only be used to return the Infosphere to a status quo after a negative influence, never to increase the well-being beyond its natural state. Together, these points suggest that cyber war is ethically justified, as long as it is to maintain the health of the Infosphere. There is a lack of guidance about how this high level ethical view can be translated into practical scenarios. Is it ethical to declare cyber war on a state if that state is suspected of developing nuclear weapons? If another state censors all information about an artist, does that mean cyber war against that state is justified? If so, it may cause an escalation of tensions into kinetic war. The abstract nature of the Infosphere presents issues, and more work is needed to help answer these questions.

In comparison to Taddeo, Lin et al. (2012) have taken a more practical approach to the ethical questions of cyber warfare by identifying a number of key aspects that need ethical consideration:

- Aggression: what kind of cyber attack counts as aggression worthy of a military response?
- Discrimination: is it possible to be precise enough with cyber attacks that collateral damage is kept minimal?
- Proportionality: what kind of responses are proportionate for particular cyber attacks?
- Attribution: the moral obligation to be correct in assigning blame for an attack.

There is some identifiable overlap with these ethical challenges. Determining what kind of attack counts as aggression overlaps with legal discussion on cyber warfare. Likewise, avoiding collateral damage and ensuring attacks are proportional are also issues which have both ethical and legal aspects. The need to correctly attribute an attack is not only morally required, but also required to retaliate legally. The answers to these ethical questions may go hand in hand with the drawing up of legal frameworks for cyber warfare.

A novel ethical aspect discussed by Lin et al. (2012) is that of perfidy. The Geneva Protocol (Protocol I of the Geneva conventions, 1977) defines perfidy as:

> "Acts inviting the confidence of an adversary to lead him to believe that he is entitled to, or is obliged to accord, protection under the rules of international law applicable in armed conflict, with intent to betray that confidence."

In other words, perfidy is deception that abuses the trust placed in the international laws of war. Examples of perfidy in kinetic warfare include impersonating the Red Cross to move troops without fear of being attacked, or the feigning of civilian, non-combatant status. Lin et al. (2012) point out that the cyber domain naturally offers methods of deception and trickery, and these need to be controlled by ethical guidelines so that perfidy is not committed. Rowe (2010) agrees with this view and puts forward an argument that hiding malware inside innocent looking code could be classed as perfidy, because it is using legitimate, civilian activity to hide military intent. It can be argued that this extends beyond just malware. Any cyber attack that attempts to hide amongst civilian internet traffic or use a civilian to carry an infected USB drive could be seen as perfidy. Just as soldiers should not hide amongst civilians, it can be argued that cyber attacks should not hide amongst civilian activity.

There are counter arguments to these points however. Firstly it can be argued that hiding cyber attacks in civilian activity does not cause any significant level of harm to those civilians. The aim of the perfidy law is to ensure continued protection of civilian populations and non-combatants (Customary International Humanitarian Law, 2005). If forces begin to distrust these groups, protection may not be as forthcoming as it would ordinarily be. This is a valid concern in kinetic warfare, but in the cyber domain the worries are less significant. If forces begin to distrust civilian internet traffic, it may be subject to closer scrutiny by firewalls and intrusion detection systems. In the worst cases, civilian internet traffic may be dropped completely by firewalls. This is an inconvenience to civilians but it is not as harmful as firing upon or imprisoning civilians due to distrust in the kinetic world. Secondly, it can be argued that perfidious-like cyber attacks are unavoidable in cyber warfare. Cyber attacks must pass through the same infrastructure used by civilians, without any special markings that designate that traffic or code as military.

NATO has published the Tallinn Manual (NATO, 2013), which provides some guidance on perfidy in cyber warfare. The manual states that combatants are not obliged to mark websites, IP addresses or other information technology facilities that are used for military purposes. However, making such entities appear to have civilian status with a view to deceiving the enemy in order to kill or injure is perfidious. Secondly, it states that while concealing the origin of an attack is not perfidious, inviting the enemy to conclude that the originator is a protected person would count as perfidy. Finally, the manual concludes that conducting cyber attacks through civilian infrastructure does not automatically make them perfidious – unless it is specifically protected infrastructure such as medical systems. The Tallinn Manual is discussed in more detail in Section 4.4.

Rowe (2010) provides a military perspective on the ethics of cyber war. He discusses issues such as ensuring civilians are made aware of what it may mean to partake in a cyber war (becoming a legal combatant, for example) and tackles the question on if fighting wars remotely can be considered ethical. He concludes by stating that cyber troops will not require physical courage, but a moral courage to do what is right without much guidance from established ethical guidelines. Dipert (2010) agrees with this view, stating that cyber warfare "appears to be almost entirely unaddressed by the traditional morality and laws of war" (Dipert, 2010).

There are currently no widely agreed ethical guidelines for cyber warfare, however researchers such as Taddeo have attempted to translate existing ethical justifications into the cyber domain. Many questions still remain on the ethics of cyber warfare and these have been raised by Lin et al. (2012). The challenge of formulating ethical guidelines for cyber warfare is an important one for the research community to overcome and is arguably the key to solving other problems. For example, laws regarding the conduct of cyber warfare cannot be put into place without first knowing what is and is not ethical conduct in this new domain. Once the ethics are agreed upon, the process of formulating laws that enforce ethical behaviour can begin. As with early warning system research, this is another topic that requires a multi-disciplinary approach, bringing together both technical and ethical minds to discuss what is possible and where ethical boundaries lie.

4.3. *Conducting cyber warfare*

When a new domain of war arises, there is an immediate challenge in determining how to operate inside of it effectively. The arrival of air as a domain of war was met with research on how its properties could be leveraged to most effectively fight in it. The same process applies to the arrival of the cyber domain. This research challenge is therefore concerned with addressing how to conduct cyber warfare, and how properties of the cyber domain shape that conduct. Parks and Duggan (2011) have examined the established principles of kinetic warfare, as defined by the US Department of Defense. They then suggest eight new principles that shape the conduct of cyber warfare. These new principles are as follows:

1. Lack of physical limitations
2. Kinetic effects
3. Stealth
4. Mutability and inconsistency
5. Identity and privileges
6. Dual use
7. Infrastructure control
8. Information as operational environment

4.3.1. *Lack of physical limitations*

In kinetic warfare, navies must travel across oceans, and ground troops must navigate terrain. This does not apply to cyber warfare and an attack can be launched from anywhere with equal impact. This view has some counter arguments however, since it can be argued that there are still some

physical limitations. Just as a navy must travel over a physical ocean, a cyber attack must travel over physical cables. The requirement of travel has not been removed, it is just the speed of travel that has increased in comparison to kinetic forces. In the case of delivering malware via USB, physical limitations also still apply in getting the USB to the required USB port. Where a lack of physical limitations is more convincing is in the production of cyber weapons. Traditional weapons require both materials and time to produce – cyber weapons do not have these same requirements, and can be replicated quickly and cheaply. Parks and Duggan (2011) give the example of the Low Orbit Ion Cannon, a cyber weapon which was freely available to download online.

4.3.2. *Kinetic effects*

The aim of cyber warfare is to cause kinetic effects. This includes physical damage or simply affecting the decision making process of an adversary. Any attack which has no real world effect cannot be considered as cyber warfare. This view can also be challenged. As our definition states, cyber warfare is the use of cyber attacks with a warfare-like intent. It is not a requirement that the cyber attack succeeds and has an effect, only that the intent behind launching it was a warfare-like one. This view can be justified by examining some real world scenarios. Country A launches a missile at country B with the intent to destroy a military base, but the missile explodes before reaching its target. Is the launching of this missile not warfare? Caution must be used in requiring kinetic effects to reach a conclusion of cyber warfare.

4.3.3. *Stealth*

Stealth in cyber warfare is different to stealth in kinetic warfare. Whilst camouflage and anti-radar shielding make up traditional stealth, cyber stealth is focused on hiding amongst legitimate traffic. This principle touches upon the concept of perfidy that was raised in earlier ethical discussion by Rowe (2010) in Section 4.2. The line between perfidy and stealth is currently an ambiguous one in the cyber domain, since cyber stealth requires the use of civilian traffic: there simply is no other form of camouflage other than pretending to be civilian or enemy traffic. Although Parks and Duggan (2011) argue that stealth in the kinetic and cyber domains are different, it can also be argued that there are similarities. Both require observation of surroundings and actions to blend in to those surroundings. For a kinetic soldier, this involves wearing colours similar to the environment such as sand or grass. Similarly, someone in the cyber domain would observe the traffic around them to also create a suitable camouflage. In both domains, the goal is to not stand out amongst the environment. Therefore, the stealth principle could be argued as being similar in both kinetic and cyber warfare.

4.3.4. *Mutability and inconsistency*

This principle reflects Parks and Duggan's view that the cyber domain is unpredictable. While a bullet will fly a certain path in reality, a cyber attack may never act the same way twice due to all the software and hardware factors involved. This principle can be challenged, since it is debatable whether mutability and inconsistency are unique to the cyber domain. In kinetic warfare, small changes in air pressure, minor imperfections on individual bullets, and human factors in aiming mean that a bullet never flies the exact same path twice. This makes kinetic warfare inconsistent and mutable, and brings into doubt the theory that cyber warfare is uniquely mutable and inconsistent.

4.3.5. *Identity and privileges*

The primary goal of a cyber attacker is to assume the identity of someone who has the access required to cause harm. Exploits aim to achieve root access, social engineering is designed to gather passwords for privileged users. This is in contrast to traditional warfare, whereby assuming identities is not a part of being able to conduct battle. It is difficult to argue against this point, since gaining access to privileged accounts is a major aspect of cyber warfare. It does, however, ignore some other aspects such as distributed denial of service attacks.

4.3.6. *Dual use*

All cyber warfare tools are dual use, having both warfare and peaceful uses. This is unlike kinetic warfare, whereby the tools are generally single use. This principle has both strengths and weaknesses. As a strength, it identifies that cyber weapons are dual use. Even tools such as distributed denial of service (DDoS) tools have a peaceful role in testing defences and improving the robustness of systems. But the idea that dual use is unique to cyber warfare can be challenged. The fact that a cyber weapon can be used to test a server's robustness is not unique to the cyber domain. In the kinetic world a new tank design will be tested by firing kinetic weapons such as bullets and rocket propelled grenades to test its robustness. Kinetic weapons can also be used for hunting, for competitive sport and even for celebration, by firing into the air. Therefore, it can be argued that the dual use principle is not unique to cyber weapons.

4.3.7. *Infrastructure control*

A significant part of cyber warfare is infrastructure control. Two groups at war in cyber space will only control a limited number of systems: their own computers and edge network devices. The rest of their traffic will pass through equipment owned by third parties such as commercial ISPs and backbone providers. Parks and Duggan state that this leaves the groups exposed to the weaknesses and wills of third parties, and that gaining direct control over infrastructure will bring advantages. This principle has merit, since having direct control over devices gives advantages to both defenders (better situational awareness and the ability to block traffic) and attackers (large bot nets allowing greater impact from attacks). However, it could also be argued that the principle is not unique to cyber warfare. Armies in kinetic wars will also seek to control infrastructure. Bridges, harbours and air fields are all infrastructure that kinetic forces may seek to secure from civilian control to better serve their warfare needs.

4.3.8. *Information as operational environment*

In kinetic warfare the physical operating environment needs to be transformed into information. In cyber warfare the operating environment is already information, and no conversion from physical measurements to information takes

place. This principle is debatable, however, since the network to be used in cyber warfare is still made up of physically existing equipment, and the targets of attacks may be physical, such as power plants or factories. In this regard, some physical measurements may require converting into information.

Looking at the principles offered by Parks and Duggan (2011), it is clear that more work is needed to better identify the features of the cyber domain that will shape the conduct of cyber warfare. Lack of physical limitations in the production of cyber weapons is the strongest factor identified so far, and will affect who can possess weapons and how many can be produced. It can be argued that there are unique cyber warfare principles that Parks and Duggan have not identified:

- **Fast weapon life cycle**: Kinetic weapons have a slow life cycle; research and development of new weapons requires tens of years, and production requires time and materials. They remain a viable weapon for many years. Cyber weapons have a much faster life cycle. Research and development to find zero day exploits takes months rather than years and replication is essentially free and instantaneous. However, a cyber weapon's period of viability is variable and always at risk. Vulnerabilities that the cyber weapon relies on may be closed by vendors at any time. Once used, the signature of the weapon can be added to detection systems and blocked. Gartzke agrees with this principle, stating that cyber weapons have a "use and lose" aspect (Gartzke, 2013). However, it can be argued that a cyber weapon's effectiveness can be lost even without use. This principle is visualised in Fig. 4.
- **Non-volatility**: Kinetic weapons are generally destroyed at the point of impact and cannot be reused. Cyber weapons do not self destruct and can be reverse engineered, as Stuxnet (Kushner, 2013) proved. This means that extra consideration must be made before launching a cyber weapon, since the technology behind it has the potential to be reused by the target. This principle may result in cyber weapons that include self destruct capabilities.

Providing more insight into this area, Liles et al. (2012) have also studied how kinetic warfare principles may be applied to cyber warfare. They examine the nine principles of traditional warfare used by the US Army (shown in Table 2), and discuss the ease of applying them to cyber warfare.

Liles et al. argue that the objective principle can be applied to cyber warfare without much work; those engaged in cyber warfare will have objectives, and launch attacks to achieve those objectives. This idea of objective agrees with our definition, since the pursuit of military objectives are warfare-like intents. Examining the offensive principle, they find difficulty in applying it to cyber warfare. They suggest that cyber space blurs the line between offense and defence and that this principle therefore cannot be applied to cyber warfare. This perspective must be challenged however, since cyber defence teams run red vs blue exercises where the idea of offense and defence are well defined. It can be argued that seizing the initiative is locating a zero day vulnerability and exploiting it before the enemy does. Retaining the initiative translates to constantly looking for new vulnerabilities, or installing back doors to ensure multiple paths into a system. Exploiting the initiative refers to fully exploiting the advantages gained by seizing and retaining the access.

Liles et al. look at mass and economy of force as one and find them challenging to apply to the cyber domain. Using an example of a DDoS attack, they claim that the force behind it is not significant, even though the effect is great. In contrast, they claim the maneuver principle is easier to apply, since operating in cyber space only makes maneuvering quicker. Rather than command large armies across vast terrain, maneuvering in the cyber domain can be thought of as quick decision making, enabled by the use of computers. They claim that unity of command is also easily applied: since IT improves command and control in traditional warfare, being immersed into an environment of IT (the cyber domain) boosts command and control. The view that command and control will improve because the environment is entirely made up of IT must be challenged, however. The replacing of kinetic forces with cyber forces may make unity of command more difficult, since attacks can be launched and counter launched in milliseconds, increasing the pace of warfare. Malware has the potential to spread and not be easily recalled or directed elsewhere. To be effective, automated defences will have to make decisions with no human input. For these reasons, unity of command may be challenging in cyber warfare.

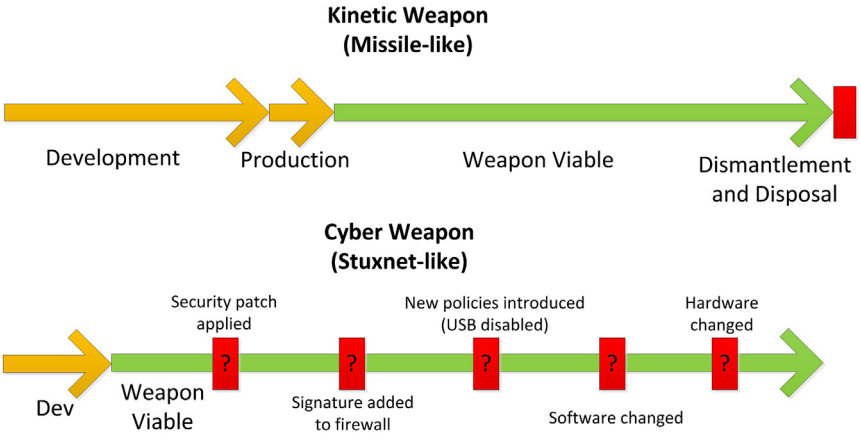

Fig. 4: – Weapon life cycles.

Table 2 – US Army principles of kinetic warfare (Liles et al., 2012).

Principle	Description
Objective	Every military act should have a clearly defined and attainable objective
Offensive	Seize, retain, and exploit the initiative
Mass	Focus the effects of combat power at the decisive place and time
Economy of force	Allocate minimum essential combat power to secondary efforts
Maneuver	Place enemies into a disadvantageous position through the flexible application of combat power
Unity of command	Ensure unity of effort under one responsible commander
Security	Never permit the enemy to acquire an unexpected advantage
Surprise	Strike the enemy at a time or place or in a manner for which he is unprepared
Simplicity	Plans and orders should be clear and concise

Regarding the security principle, they suggest that avoiding unexpected advantages in the cyber domain is difficult. Even if perfectly secure systems are designed, an insider attack may still present an unexpected advantage for an opponent. However, it can be argued that this principle can be adapted. Instead of aiming to never allow unexpected advantages for the enemy, it should be translated to minimising the opportunity for and impact of unexpected advantages. This modification allows for the fact that unexpected advantages will arise as new vulnerabilities are discovered, but gives cyber defence teams the aim of minimising the impact of those advantages.

To follow the surprise principle, Liles et al. argue that cyber attacks should target systems where they are least expected. This is because these systems will likely have the weakest protections and monitoring. In addition to Liles et al.'s suggestion, it can also be argued that surprise includes using cyber weapons that can remain stealthy. By using sleeper malware that hides in a system and activities upon receiving a signal, the principle of surprise can be applied.

Applying simplicity to cyber warfare, they claim that there is nothing simpler than the one or zero of binary. While this is true, Liles et al. may have misunderstood the intent behind this principle. Whether ones and zeros are simple or not does not reflect the purpose of this principle, which is to ensure plans and orders are simple enough to be carried out as intended. In the cyber domain, this simplicity translates to giving clear orders such as securing root access on a particular host.

Both Parks and Duggan (2011) and Liles et al. (2012) have attempted to identify principles by which cyber warfare can be conducted, but both have encountered challenges. Weaknesses were identified in the suggested principles and the arguments behind them.

Laprise (2006) has offered a different perspective into the area of conducting cyber warfare by comparing it to naval warfare.

Fig. 5 shows five strategic principles, along with how each would be represented in both maritime and cyber warfare. Laprise states that all of the principles have easily identifiable

Strategic Principle	Maritime Example	Cyberspace Example
Decisive Battle	Fleet Battles	None-Inability to cause irreparable harm
Siege	Blockade	Denial of Service Attack
Area Control	Aircraft Carrier Defense	Webmaster Vigilance
Area Denial	Aerial Patrol and Surveillance	Compromised Website
Commerce Warfare	Submarine Warfare	Hacking

Fig. 5 – : Laprise's comparisons between maritime and cyber warfare (Laprise, 2006).

examples in the cyber domain, except for one: decisive battle. Laprise finds difficulty in finding a cyber equivalent of a decisive battle, since while operating systems may be wiped, there is no permanent physical damage to the hardware and therefore cyber warfare alone cannot win a war. This is in agreement with authors such as Gartzke (2013), who argue that cyber warfare must operate alongside kinetic warfare to have any decisive meaning. There are challenges to this view, however, since there are imaginable scenarios where cyber warfare could inflict a decisive blow. Continuing the maritime theme, malware that can simultaneously disable weapon systems on all battleships may be decisive enough to cause surrender. However, the argument still remains that this disablement would likely be temporary in nature and only decisive when followed up with kinetic warfare.

The topic of how to conduct cyber warfare and the principles that shape it is a challenging one. Authors such as Parks and Duggan (2011) have taken the approach of trying to identify what the principles of cyber warfare may be. But as has been demonstrated, their arguments often have counter points that bring the usefulness of the principles into question. Others such as Liles et al. (2012) have taken existing principles and attempted to translate them into the cyber domain, but with limited success. Laprise (2006) took another approach, attempting to compare the better understood domain of sea and make comparisons with the domain of cyber. It must be concluded that there is no satisfactory set of cyber warfare principles currently available. It is unclear if future academic research can address this gap, or if it is a problem that can only be addressed through experience of cyber warfare. The first aircraft used in early air warfare did not come with a set of air warfare principles, they were developed based on the experiences of air warfare pioneers. In this regard, the emergence of true cyber warfare principles may rely on the experiences of cyber warfare pioneers.

4.4. *Applying existing laws to cyber war*

With a long history of war, the world has seen the development of long standing and internationally accepted laws on

how traditional kinetic war should be carried out to remain legal (US Dept of Defence, 2012). With cyber warfare being sufficiently different from kinetic warfare, attempts to apply the laws of armed conflict to cyber warfare have presented a new research challenge. Questions on who is a legal combatant, state neutrality and the protection of civilians all need to be answered by this research area. The most comprehensive work on this topic comes from NATO in the form of the Tallinn Manual (NATO, 2013). Put together by an international group of experts, the manual is not a lawfully binding document but gives guidance on how existing laws of armed conflict apply to cyber war. It is out of the scope of this paper to analyse all 95 rules from the document, but an overview and some analysis on the overall approach of the manual can be given. The structure of the Tallinn manual is shown in Fig. 6.

As an example of the manual's approach, rule 43 addresses indiscriminate means or methods. The rule states that:

> "It is prohibited to employ means or methods of cyber warfare that are indiscriminate by nature. Means or methods of cyber warfare are indiscriminate when they cannot be: a) directed at a specific military objective or b) limited in their effects as required by the law of armed conflict and consequently are of a nature to strike military objectives and civilians or civilian objects without distinction."

The manual explains the legal basis for this rule, citing Article 51(4) (b) and (c) of the Additional Protocol I of the Geneva conventions (1977). The group of experts also give examples of what would and would not violate this rule. For example, a piece of malware that could not be controlled and would harmfully spread beyond its intended target would violate the rule. However, Stuxnet-like malware which spreads into civilian systems but only attacks very specific equipment would not violate the rule. This methodology of

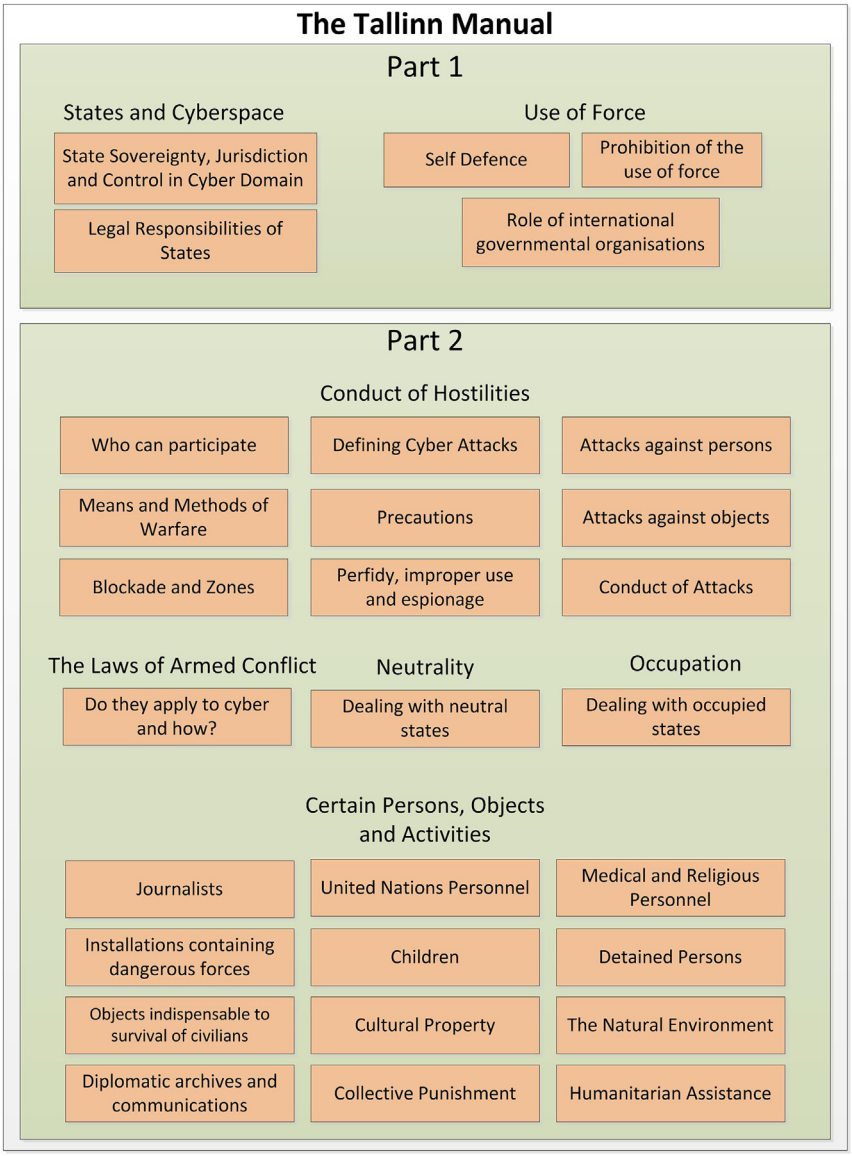

Fig. 6 – : Overview of the structure of the Tallinn Manual.

Table 3 – Schmitt analysis (NATO, March 2013).

Factor	Description
Severity	Attacks that cause physical damage or injury are more severe than those that just disrupt operations, and are more likely to be seen as a use of force
Immediacy	A quick attack that leaves no time for a peaceful response is more likely a use of force
Directness	An attack which has a direct effect such as an explosion is more likely to be seen as a use of force than one which has a more indirect effect such as a slowing of the economy.
Invasiveness	An attack which penetrates an important military system is more likely a use of force than one which penetrates a small business
Measurability	The more quantifiable the effects of an attack, the more likely it is to be seen as a use of force
Presumptive Legality	If there is no specific law against something, it is considered legal and therefore not a use of force

rule, basis and explanation is followed throughout the manual, making it easy to follow how the group of experts developed each rule and the legal reasoning behind it.

Although the manual is detailed and arguably the best attempt yet to translate the existing laws of armed conflict into the cyber domain, it does have weaknesses that need to be addressed. Firstly, the manual admits that to produce the rules, only the military manuals from four countries have been used: Canada, Germany, the United Kingdom and the United States. This means that the manual may potentially be biased and influenced by western thinking of war and conflict. Other organisations such as the Shanghai Cooperation Organisation (SCO) have shown an interest in regulating cyber warfare and a collaborative effort between the SCO and NATO would arguably produce more globally acceptable results. Secondly, the group of experts encounter issues when trying to translate terms such as the "use of force" into the cyber domain. Determining when a "use of force" has occurred is of great importance, since it defines the moment that a state has violated the UN Charter. Rule 11 attempts to define the use of force in the cyber domain, but concludes that whether "force" is used in a cyber attack is subjective and dependant on a Schmitt Analysis, as shown in Table 3. Even with the detailed and valuable work of the Tallinn manual, a state coming under cyber attack still has no conclusive guidance on if the attack is a use of force or not.

A final significant issue with the manual is that the group of experts rarely reach a unanimous agreement on how the laws should be applied in the cyber domain. Many rules printed in the manual state that a certain number agreed with aspect A, whilst another number disagreed. This highlights the difficulty encountered in translating the existing laws, rather than a failing of the manual.

Michael Schmitt is an active researcher in the area of international law and cyber warfare (Schmitt, 2012a, 2012b, 2012c, 2012d) and was director of the International Group of Experts involved in writing the Tallinn Manual. Schmitt (2012d) compared the Tallinn manual against a speech by US State Department legal advisor Harold Koh (2012). This speech was regarded as significant, since it set out the United States' view on how laws applied to the cyber domain. Schmitt concludes that in the majority of points, the Koh speech and Tallinn Manual are in agreement. Both conclude that a cyber attack can be classed as a use of force in some circumstances, both agree that states may act in self defence and so on.

Foltz (2012) has studied Stuxnet (Kushner, 2013) to help define what can class as a use of force in cyber space. He concludes that in most respects, Stuxnet meets the requirements to be classified as a use of force, but an obstacle to doing so is the attribution problem. Without being able to attribute a particular attack to a nation state, Foltz claims that uses of force in the cyber domain are difficult to prove. He concludes that those involved in cyber warfare have to be prepared to operate in an ambiguous and contested legal environment until the domain has matured.

Fanelli and Conti (2012) have also used the Stuxnet scenario to examine if international law can be applied to cyber attacks. In particular they attempt to apply the principles of discrimination, distinction and proportionality. They conclude that Stuxnet showed discrimination and distinction. While it propagated to as many machines as possible, the primary payload was only launched if it located a very specific target. The attack also showed proportion, since it made small but effective changes to the operation of centrifuges, causing them to fail safely with little to no collateral damage. This work therefore supports the view that international law can be applied to the cyber domain.

Rauscher and Korotkov (2011) take an alternative approach by arguing that the process of conversion needs to be made easier before it can be successful. They present five recommendations that would make applying existing law to the cyber domain easier:

- **Detangling protected entities in cyberspace**: The separation of civilian and military systems.
- **Application of the distinctive Geneva emblem concept in cyberspace**: Marking of protected zones, e.g. medical systems.
- **Recognizing new non-state actor and Netizen power stature**: Recognising that non-state actors may be involved in cyber warfare.
- **Consideration of the Geneva protocol principles for cyber weaponry**: A suggestion that cyber weapons need to be understood before laws can be made.
- **Examination of a third, other-than-war mode**: Classifying cyber warfare as something different, avoiding the need to adapt existing rules.

These recommendations are useful in that they present a novel approach to applying existing law to cyber warfare. While other authors focus strictly on how the laws translate,

these recommendations suggest how this translation could be made easier. Some of the ideas are difficult to achieve technically (such as having marked zones and detangling civilian and military systems), but they offer a good basis for future research.

To summarise this research area, there is a challenge in applying the established laws of armed conflict to cyber warfare. Aspects such as the use of force, self-defense and ensuring attacks are discriminate are all issues that have led to debate when it comes to applying them to the cyber domain. The Tallinn Manual offers the most comprehensive guide yet on how the laws apply, but does not solve all of the issues. The international group of experts could not reach a definitive answer on when a cyber attack constitutes a use of force or when the right to self-defense should be granted. As has been stated, a full examination of the rules given by the Tallinn Manual is out of scope for this paper, but these examples highlight the lack of legal guidance on how international law applies to cyber warfare. As Foltz stated, nations should be prepared to conduct cyber warfare under ambiguous guidelines and legal grey areas for the foreseeable future.

4.5. *Cyber weapons*

The topic of cyber weapons covers a range of challenges: defining what a cyber weapon is, how they are different to traditional weapons, if it is possible to control their production and use and so on. Arimatsu (2012) has defined a traditional weapon as "a device designed to kill, injure, or disable people, or to damage or destroy property". She argues that this definition is not suitable for cyber weapons, since the purpose of a cyber weapon is often to cause an indirect kinetic effect, that may or may not result in death, injury or damage. In other words, cyber weapons such as a piece of malware may have the goal of simply enabling the collection of data or opening a backdoor for future attacks. Arimatsu also rejects the idea that a cyber weapon could be defined by its potential to inflict harm, stating that such a definition is too broad. She examines the idea that a cyber weapon could be defined as malicious software that possesses an offensive capability, but points out that this is not specific enough to allow legal regulation, due to the dual use nature of tools and code. Arimatsu concludes that to define cyber weapons, both capability and intent need to be examined together. Therefore, a piece of malware or a tool only becomes a cyber weapon when it has the capability to cause harm, and the person using it has a harmful intent.

This definition addresses the dual use issue, and agrees with our definition model that intent is a vital aspect in defining cyber terms. Evidence supporting the need for intent can be found by examining comparable kinetic events: A knife in the hands of a chef is a tool, but when the user of the knife gains harmful intent, the tool becomes a weapon.

The issue of controlling cyber weapons is also a research challenge. Denning (2000) argues that with well established international controls over the production and trade in kinetic weapons, it is only natural to investigate whether the same controls should apply to cyber weapons. She concludes that regulating the production and trade of cyber weapons would have some advantages including a reduction in the number of cyber attacks, sending a message that cyber weapons are unacceptable and easing international tensions regarding cyber attacks. Denning points out that creating cyber arms controls encounters a number of obstacles however:

- Difficulty of enforcement
- Reaching international agreement
- Defining acceptable limits of activity
- Poor cost effectiveness of regulation
- Impact on free speech
- Reduced capacity for nations to retaliate

Arimatsu (2012) has examined the potential for cyber arms control treaties in detail. She describes how there are broadly four types of treaty:

- Limiting the number of specific weapons in the world
- Restricting the use of specific weapons
- Restricting the testing of specific weapons
- Restricting the development and acquisition of specific weapons

It can be argued that limiting the number of cyber weapons is not a realistic prospect, since code can be replicated and copied in fractions of a second at a tiny computational cost. Restricting the testing of cyber weapons is also a difficult task. Unlike a nuclear weapon, a cyber weapon can be tested on a private network with no evidence of testing detectable by a third party. Restricting the development and acquisition of cyber weapons is again not a feasible goal: malicious code can be written from scratch or copied and sold to third parties. Encryption techniques could also hide the transport of cyber weapons between seller and buyer. Therefore, the only viable type of treaty is one that restricts the use of specific cyber weapons. Nation states agreeing to such a treaty would be prohibited from using certain types of cyber weapon, such as those which do not discriminate between civilian and military targets.

Arimatsu points out that it is important to look at the overall goals of arms treaties, to see if the same kind of goals can be achieved in the cyber domain. She suggests that traditional arms control treaties have the following goals:

- Minimising disparities in arms levels between states to reduce instability
- Increasing predictability in relations between potentially hostile states
- Pre-empting the development of new weapons
- Decreasing global expenditure on arms to divert funds to economic and social causes
- Fostering a non-hostile atmosphere
- Decreasing suffering and damage during armed conflict

The majority of these overarching goals are aimed at maintaining a balance of power between nation states. Arimatsu notes that this is a valid goal when such weapons are only affordable to states, but that when it comes to very cheap cyber weapons which can be obtained by anyone (including non-state actors), the notion of maintaining a balance of power in the cyber domain is not a convincing one.

Arimatsu concludes that there are a number of other obstacles preventing the creation of effective cyber arms control treaties. Firstly, she states that the pace of technology is so great that any list of banned cyber weapons would be obsolete within days. A ban list would have to describe effects and characteristics that cyber weapons must or must not have, and would be general in nature. Secondly, she is in agreement with Denning (2000) that verifying compliance would be an almost impossible task. Whilst hiding chemical weapons from inspectors is a relatively difficult task, cyber weapons could be just a few bytes of data, stored in the cloud and encrypted. Even if inspectors did find a banned tool or piece of code, the dual use aspect means that without proven intent to use it for harm, it is not a cyber weapon.

Rowe (2010) identifies three specific challenges posed by cyber weapons:

- Collateral damage
- Unpredictability
- Damage assessment

He states that there are a number of reasons why cyber weapons may be more prone to collateral damage than kinetic weapons. Firstly, he argues that in the cyber domain, civilian and military targets are hard to distinguish. This idea relates to the work discussed previously by Rauscher and Korotkov (2011), who proposed an attempt to de-tangle military and civilian systems. Secondly, he suggests that the cyber domain presents a temptation to use civilian infrastructure as stepping stones. However, it can be argued that the use of civilian infrastructure is more than a temptation: it is a necessity. This is because backbone providers that provide core connectivity to a nation are run by civilian organisations. A third factor leading to collateral damage is uncontrollability. Malware will be designed to spread automatically according to its coding, and could spread beyond its intended target.

Rowe (2010) claims that a second challenge is unpredictability: network, hardware and software issues can alter the impact a cyber weapon has. Applying a security patch or changing firewall rules could foil years of development on a cyber weapon, or make it act in an unintended way, a problem not encountered by kinetic weapons. This is a similar argument to that made earlier by Parks and Duggan (2011) that cyber warfare is unpredictable, and the same counter argument applies. Kinetic weapons are not predictable either: soldiers can encounter weapon jams, and bombs can fail to detonate upon impact. It can be counter argued that a more convincing concept is that of unpredictable impact. Assuming a bomb is dropped on an air base, there are a finite range of impacts, from destroying some aircraft to making the runway unusable. Launching a cyber attack at that same air base has a wider potential range of impacts that are more difficult to plan for. For example, malware placed into the control tower may spread beyond the airbase to other control towers, both military and civilian.

This problem of unpredictable impact is related to the third challenge: damage assessment. In most cases, the damage from a bomb dropped by an aircraft is relatively easy to assess, since it has an immediate kinetic effect that can be observed. Damage from a cyber weapon is less easy to observe. If an attacker launches a piece of autonomous malware, the effects are not immediately apparent. The extent to which it has spread is challenging to measure. The victim may also find it difficult to perform a damage assessment, since the effects may be subtle, dispersed across many systems and designed to avoid detection. Rowe highlights how negative effects of a cyber weapon such as a slowing down of a device may persist for years after the conflict, analogous to the use of land mines in kinetic warfare.

He concludes that future cyber weapons need to be controllable, in that the attacker retains control over the weapon and is able to remotely disable it. Rowe also argues that cyber weapons should contain a signature, which identifies the attacking nation. He argues that this is to abide by international law stating that all combatants must wear identifiable markings. This view is similar to Rauscher and Korotkov's view that protected zones should be marked. The Tallinn Manual disagrees with this view, however, stating that websites, IP addresses and other information technology facilities do not need to be marked. It can be argued that the Tallinn Manual is correct on this debate. Attempting to bring the concept of identifying emblems to the cyber domain is a hugely challenging task with both organisational and technical issues. How would warfare IP addresses be identified as such? Would a compromised system have to be marked as military before being used as a stepping stone? With these questions in mind, it becomes apparent there are many obstacles to overcome before such a system would be useful.

Related to Rowe's call for cyber weapons to be controllable, Tyugu (2012) has examined the challenge that automated malware and anti-malware systems present. Automated malware will attempt to find the best targets and attack vectors, whilst anti malware systems will increasingly act autonomously to defend systems. According to Tyugu there are three dangerous situations that automated malware and anti-malware systems may encounter:

- Misunderstanding of a command
- Misunderstanding of a situation
- Unexpected emotions

Misunderstanding of commands arises when the protocols used between automated agents are not verified well enough. Semantic problems of understanding may arise between automated agents, which could lead to unsuitable actions being performed. Misunderstanding of a situation relates to the problem whereby an event occurs and the automated malware or anti-malware reacts in an undesirable way due to having an incorrect view of the situation. While automated systems do not currently have emotions, they can prioritise actions that are more urgent than others. These priorities may conflict or result in undesirable behaviour in response to a complex situation. A final threat raised by Tyugu is the formation of unwanted coalitions between autonomous malware. As an example, malware inside of a botnet may communicate with other nodes and collectively decide the best way to achieve a goal. This kind of collective decision making between multiple autonomous cyber weapons may lead to undesirable actions and a loss of control by human operators. It can be argued that concern over automated cyber

weapons is warranted. With cyber attacks able to be delivered in milliseconds, the temptation to automate systems increases. This damages the earlier discussed principle unity of command, and removes the ability of a human operator to direct and if necessary, disable the cyber weapon from causing further damage. This view is supported by Caton (2013), who states that automated cyber weapons remove human decision making and could turn a bad situation into a catastrophic one.

In summary, the area of cyber weapons presents many research challenges. Arimatsu and Denning have asked if cyber weapons can be subject to arms control, and both agreed that there are difficulties in applying traditional concepts of arms control to the cyber domain. The issue of controllability is also an issue. Automation of cyber weapons and cyber defenses will be a tempting prospect for nations, but researchers such as Tyugu, Rowe and Caton have warned that this automation needs to be balanced with control to avoid situations where cyber weapons reach beyond the ultimate control of a human operator. As with the other challenges presented in this paper, the challenge presented by cyber weapons needs to be addressed by a multi-disciplinary approach. Computer science, ethics, law and military input is required to assist in shaping the future of cyber weapon use.

4.6. *Attribution problems*

Attribution is defined by Wheeler and Larsen (2003) as "determining the identity or location of an attacker or an attacker's intermediary". Authors such as Wheeler and Larsen have argued that attribution is an essential element of cyber warfare, claiming that: "As with conventional warfare, a good offense is often the strongest defense. However, many offensive techniques, such as computer network attack, legal action (e.g., arrests and lawsuits), and kinetic energy attacks, can only be deployed if the source of the attack can be attributed with high confidence" (Wheeler and Larsen, 2003). This view is supported by Dever and Dever, who state that cyber defense models "rely heavily upon the advancement of technological capability to assist with the ever vexing issue of attribution" (Dever and Dever, 2013). Friesen (2009) agrees, stating that the inability to attribute a cyber attack stands in the way of regulating cyber warfare.

However, the view that attribution is essential in cyber warfare is challenged by other authors such as Hare (2012). He counter argues that lacking absolute attribution of a cyber attack is not a barrier to a nation responding. Hare suggests that the politics between nations is dynamic enough so that reasonable suspicion of responsibility can be enough to initiate a retaliatory response. An example given by Hare is of a nation aggressively lobbying for positions that conflict with interests of the suspected attacker on the international stage. As long as the suspected attacker realises that this hostile political positioning is in response to the cyber attack, the victim has managed to effectively respond to the attack without unequivocal attribution.

Looking at these arguments, it can be argued that the importance of attribution is diminished but not eliminated in cyber warfare. While states may not require absolute attribution to make a response, strong attribution will likely be useful for arbitration on the international stage, in forums such as the United Nations.

A major challenge in the area of attribution is that of prepositioning. Wheeler and Larsen (2003) present seventeen attribution techniques, but claim that they require prepositioning of both trust and technology. Logs cannot be studied if the technology to keep those logs was not prepositioned before the cyber attack occurred. Similarly, network administrators cannot work together effectively to find the source of an attack if the trust relationship between those administrators and their organisations is not prepositioned. Setting up these trustful relationships between organisations can be difficult: differing languages, conflicting laws and commercial rivalry all introduce obstacles to forming prepositioned trust.

Wheeler and Larsen suggest that the obstacle of prepositioning both trust and technology can be overcome by the adoption of industry standards. By having access to a standardised set of tools that provide a legally agreed level of attribution ability, the barrier of manually creating trust relationships between organisations is removed, since the technology and trust would be prepositioned by default.

Boebert (2010) has challenged the view that having standards would end the attribution problem, since technical attribution alone is not a useful legal tool. An IP address cannot be held responsible for a cyber attack, and even if that IP address is traced to a physical machine, the owner of said machine can claim it was stolen, used by a visitor or taken over by malware and used remotely. He therefore argues that technical attribution needs to be converted into human attribution: proving that a human being performed action A at time B. To do this, he suggests keystroke analysis could be used. It can be argued that this solution is weak, however, since using keystroke analysis for attribution has problems. Firstly, the attack may not require "live" typing, so there are no markers such as speed to measure against. Secondly, even if live typing was used, logs would not be able to show the speed or the number of errors – only the final command after enter was pressed. Thirdly, a suspect who has their typing monitored as part of an investigation may intentionally alter their keystroke behaviour.

The area of attribution is vast, and spans not just cyber warfare but also other areas such as cyber crime. As stated earlier, there are many papers from the research community that examine the technical aspects of how to perform and improve attribution of cyber attacks in general (Clark and Landau, 2010; Hunker et al., 2008; Kalutarage et al., 2012), and specifically for critical national infrastructure (Nicholson et al., 2013). While attribution is clearly very important in other areas such as cyber crime, it has been argued that it is of lesser importance in cyber warfare because absolute attribution is not necessary to elicit a retaliation. Others insist that ability to attribute attacks continues to be a major challenge for cyber warfare. More research would be useful to not only continue improving attribution methods, but to also reach conclusions on just how necessary it is in cyber warfare.

4.7. *Cyber defence and deterrence*

This area of research is focused on two main questions: How does an entity defend itself from cyber attacks, and how can it

deter an aggressor from launching cyber attacks in the first place? As with attribution, these two questions not only apply to cyber warfare, but also more broadly to all forms of cyber attack. Saydjari (2004) argues that a good cyber defence system requires six elements:

- **Sensors and exploitation**: The eyes and ears of a defence system, detecting attempted attacks.
- **Situational awareness**: Converting sensed attacks into meaningful data from which decisions can be made.
- **Defensive mechanism**: Technology that counters cyber threats. E.g. antivirus software.
- **Command and control**: Making and executing defensive decisions quickly and effectively.
- **Strategies and tactics**: Knowing which defensive actions are best, and when a change in actions is beneficial.
- **Science and engineering**: An understanding of how to design and improve defensive systems.

This is a comprehensive view of cyber defence, but it can be argued that a seventh element is missing: cyber intelligence. Cyber intelligence would address the element of learning from past attacks and incorporating lessons learnt into each and every stage. For example, if a cyber attack does defeat a defence team and cause damage, time needs to be spent working out which elements needs to be hardened to prevent that attack in the future: Was it missed by the cyber sensors and could they be hardened to prevent that happening again, or was it a fault in the cyber strategies and tactics? Perhaps the sensors and strategy were fine, but the actions were taken too slow, meaning that command and control requires strengthening. The crucial element of early warning is also missing, as was discussed in Section 4.1.

Saydjari (2004) states that there are a number of research challenges that remain unresolved in the area of cyber defence. He calls for more research on a variety of topics including how to make trustworthy systems out of untrustworthy components, better intrusion detection technology, and better ways of responding to distributed denial of service attacks. He concludes by putting forward an argument for a national cyber defence capability in the US: A government led, concentrated national effort to gather the best minds and formulate an effective cyber defence policy. Saydjari (2008) argues that the national effort will require the cooperation of a number of government agencies, an extensive budget, and the support of the U.S. President.

Fernández Vázquez et al. (2012) suggest an alternative approach, emphasising the importance of information sharing networks between organisations as an effective way to bolster cyber defence. They examine why previous attempts at information sharing networks have failed, and how to ensure they succeed in the future:

- **Incentives and barriers to information sharing**: Discuss expectations with participants – why is the sharing network needed? What will be shared?
- **Information value perception and collaborative risk management**: Ensuring that participants see value in the information shared and share an appreciation of how that information impacts risk in their organisation.
- **Improving data exchange**: Formulating agreed paths of information flow, to ensure information reaches relevant individuals in each organisation.
- **Automation of sharing systems**: Encouraging automation to speed up the sharing of information and provide it in a standardised form.

O'Connell (2012) provides another perspective on cyber defence, stating that it can be improved through education on what she terms "good cyber hygiene". Rather than create complex defence systems as Saydjari (2008) has suggested, or rely on information sharing agreements between organisations as highlighted by Fernandez Vazquez et al. (2012), O'Connell argues that most cyber attacks can be prevented by simply educating users of information technology so that they can avoid assisting an attacker. This viewpoint has merit, since Stuxnet was given access to its target via an employee inserting a USB drive into a control network (Kushner, 2013). It can therefore be argued that educating people on security issues is a significant part of cyber defence.

Richard A. Clarke, who was special advisor on cyber security to president Bush (2001–2003) presents a view held by some private organisations that defending from cyber warfare is a job that governments should be doing. He provides an analogy, stating that asking private organisations to self defend themselves from cyber warfare is like asking them to install their own anti aircraft platforms at their businesses (Clarke and Knake, 2010). This view can be challenged however, since there are significant differences between a kinetic defence and a cyber defence. Defending from a kinetic attack such as an air strike requires hardware that is restricted in sale and expensive. It is also a task that involves specific military knowledge and expertise: What type of aircraft will likely attack? What altitude will they be at, and what countermeasures do they have? These are questions of a purely military nature that the military is best positioned to answer. With cyber defence however, the same defences used to counter a criminal cyber attack can be used to help counter cyber warfare. Therefore, it can be argued that it is not unreasonable to ask private organisations and individuals to take a role in defending themselves during cyber warfare. Counter arguments to this point are that firstly, cyber warfare attacks may be so sophisticated that standard defences are not sufficient. Secondly, asking civilians to take part in defending from cyber warfare raises legal questions on combatancy.

The second aspect of this sub topic is that of deterrence. While cyber defence is concerned with stopping attacks being successful, deterrence is concerned with discouraging the aggressor from launching the attack in the first place. Libicki defines cyber deterrence as "a capability in cyberspace to do unto others what others may want to do unto us" (Libicki, 2009). In other words, cyber deterrence is ensuring that adversaries know that if they launch a cyber attack, they will get a cyber attack back. Libicki highlights how deterrence has been proven successful in the past. Nuclear deterrence helped ensure that the cold war between the United States and Soviet Union never escalated into a hot war (Powell, 1990). But Libicki argues that when it comes to cyber deterrence, there are some challenges to be resolved:

- **Attribution**: If the attacker believes they will not be traced, the threat of retaliation is not a deterrence.
- **Failure to recognise risks**: The attacker may underestimate the cyber ability of those they are attacking, or overestimate the security of their own systems. If there is a failure to recognise the risk to their own assets, the effect of cyber deterrence is low.
- **Repeatability**: Kinetic responses such as missile strikes can be used repeatedly as required as retaliation for every attack. But cyber weapons are more prone to being single use; once a zero day exploit is used, the enemy has the opportunity to close the vulnerability. This threatens the credibility of long term cyber deterrence.
- **Setting thresholds**: It is unclear what kind of action in cyber space crosses the threshold to trigger a retaliatory response.
- **Escalation**: Retaliation in cyber space needs to be considered carefully to avoid escalating conflict needlessly. This aspect is linked to the setting of thresholds.
- **Cyber dependence**: If a nation has very little cyber infrastructure, the effect of cyber deterrence is low since they have little at risk. Clarke and Knake (2010) agree that this is a major challenge facing cyber deterrence.

Most significantly, Libicki (2009) argues that there is an underlying problem with the whole concept of cyber deterrence. He states that while a nuclear deterrent threatened to cripple a nation, a cyber deterrent does not. He therefore suggests that a cyber deterrent is only effective if it is not used, since using it would show how weak the response was. This argument can be countered however, since attacks on critical national infrastructure could cause immense harm if conducted with enough skill and resources. It can also be argued that traditional deterrence also had the same weakness: Although the superpowers threatened mutually assured destruction, it was never guaranteed that a superpower would actually carry out a retaliatory attack, or had enough weapons to make it crippling. In this respect, it can be counter argued that perceived threat rather than actual threat is what makes deterrence valuable, and that this is not unique to cyber deterrence.

Alperovitch (2011) is more convinced than Libicki (2009) that cyber deterrence can work. He agrees that attribution is a problem, but in agreement with Hare (2012) states that accurate attribution is not necessary, and that reasonable suspicion is all that is needed. He claims that states should publicly declare "red lines", which when crossed will initiate a counter strike against all suspected attackers. Recent events have shown that publicly declaring red lines can be a dangerous act however. In 2013, US president Barack Obama announced that Syrian use of chemical weapons was a red line that if crossed would provoke a reaction from the United States. This may have been intended to act as a deterrent, but when chemical weapons were used, America's will and capability to act on that red line was publicly tested (Cohen, 2013). With these announced red lines and some public demonstrations of cyber attack capability, Alperovitch claims that deterrence can play an effective role in cyber defence.

Sterner (2011) agrees that the biggest problem facing cyber deterrence is knowing who attacked and finding suitable targets to retaliate against. He points out that if the attacker is a non-state actor, retaliation may involve infringing the sovereignty of a state, a step that has greater cost than benefit. While authors such as Libicki (2009) find the concept of cyber deterrence lacking, Sterner suggests that it is simply looked at in the wrong way. He argues that deterrence is too often seen in the nuclear sense, an all or nothing situation where a use of force marks the failure of deterrence. But Sterner (2011) suggests that in the cyber domain, cyber attacks peak and trough at varying levels of intensity over a long period. In this respect, Sterner puts forth the view that entities should use deterrence in a much more dynamic way, which he calls "active-deterrence": using combinations of threats and retaliatory attacks to best manage the situation and influence events to best serve them. Sterner suggests that active deterrence may be the best kind of deterrence for the cyber domain and that rather than being the first and last line of defence, it should be seen as one measure in the bigger picture. Education on cyber security, better cooperation between organisations and improved technical security will all sit aside deterrence to form a complete package of cyber defence.

Gartzke (2013) argues that the concept of cyber deterrence is not at all convincing. He agrees that cyber weapons have short periods of viability – what he calls a "use and lose" aspect whereby the use of a cyber weapon reveals the vulnerability, damaging its future effectiveness. He gives the example of a state deterring attacks by threatening to shut down the attacker's mobile phone networks. Without proof of this ability, nations will be dubious of its actual threat, yet if it was demonstrated, the vulnerability would be revealed and the weapon would become obsolete. Again, it seems that perceived threat is what makes deterrence valuable, but the difference highlighted by Gartzke is that cyber weapons completely rely on imagined threat with no demonstrated threat at all. This can be related to the idea of sleeper malware, whereby a state may deter attacks by suggesting they already have malware inside another nation's infrastructure and could disrupt it at will.

A significant point to note is that the majority of research on cyber deterrence is centred on state versus state conflict. Authors such as Alperovitch (2011) and Sterner (2011) acknowledge this, stating that more research is needed to determine how cyber deterrence can be used against non-state actors. Dogrul et al. (2011) have come closest to taking on the non-state actor issue by looking at how cyber defence and deterrence can be applied against cyber terrorism. They begin by examining the motivation for terrorists to use cyber attacks, citing the low cost, anonymity and lack of physical barriers. They conclude that there are two approaches to defending from non-state actors. Firstly, there is a legislative route. This involves the creation of a "robust, international legal framework under the UN" (Dogrul et al., 2011) which will raise the risk of carrying out an attack due to an international response rather than a response by just the attacked state. Secondly, they argue that a military aspect is also needed. They call for cyber defence teams to be created at organisations such as NATO, whose powers include being able to perform counter cyber attacks against identified non-state aggressors. There are however weaknesses in this approach, in that not all nations are members of NATO. If attacks

originate from a non-member state, questions are raised on how effective a NATO cyber defence team could be in acting as a deterrent. The attribution problem also still remains unsolved: if the attackers feel they cannot be traced, a NATO cyber defence team will present little deterrence.

The topic of cyber defence and deterrence is a complex one. Applying traditional principles appears to be difficult, since the aggressor can often remain unknown. As stated by Hare (2012), attribution may not always be necessary in politics, but when it comes to cyber deterrence it is arguably essential because the principle of deterrence relies on the attacker fearing retaliation. While deterrence has been a strong tool in traditional defence, it can be concluded that in the cyber domain deterrence is best regarded as just one tool amongst many. Other tools such as building cooperation between organisations and nations, education and better security are key to creating a well rounded cyber defence, alongside deterrence. In this respect, the concept of deterrence is perhaps best seen as part of a "defence in depth" strategy.

4.8. *Nation's perspectives*

When considering cyber warfare, it is important to not only examine academia's approach. As the primary practitioners of warfare, understanding the approaches taken by nation states is a research challenge. A point that is clear from the literature, is that nations are alert to the issue and are working to formulate their individual approaches and doctrines. The United States Department of Defense has publicly announced its recognition of cyberspace as an operational domain in which it must organise, train and equip (United States Department of Defense, 2011). Joint Publication 3–13 (U.S. Joint Chiefs of Staff, 2012) describes how the U.S. has placed cyberspace operations under the umbrella term of information operations, which includes other aspects of warfare such as electronic and psychological operations. In this regard, it can be argued that the U.S. sees cyber warfare as just one tool amongst many that can support a war.

Other nations have also been active in developing their own cyber warfare doctrines (Billo, 2004). The literature shows that there are both similarities and differences in how various nations are approaching cyber warfare. Thomas (2009) has shown how the Chinese government has declared that both the army and civilians must work together to secure the nation from cyber attacks (Thomas, 2009). An almost identical encouragement towards both military and civilian effort can be seen in the United States' approach (United States Department of Defense, July 2011). Similarities in publicly declared doctrines are relatively easy to identify – a deeper challenge facing researchers in this area is in identifying differences and the reasons behind them. Thomas (2009) argues that one such difference is the focus on cognitive attacks in the cyber domain. He states that Russia in particular places cognitive attacks at the centre of its cyber doctrine, aiming to understand the enemy's thought process and then presenting actions and apparent intentions that seek to exploit that understanding, allowing the enemy commander to reach a decision favourable to Russia. He suggests that China also considers cognitive cyber issues in its doctrine, but that such concepts are less central to US doctrine. Billo (2004) agrees with this view, stating that "The U.S tends to focus on the computer network attack aspects of cyber warfare but Chinas cyber warfare focuses more on psychological operations and denial and deception of military data" (Billo, 2004). Billo puts forward further differences in approaches between China and the United States. He highlights how Chinese cyber warfare doctrine contains references to Sun Tzu's (2005) principle of subduing an enemy without battle. Thomas (2009) has also made this observation, stating that the Chinese approach to cyber warfare encourages pre-emption and the idea of maintaining dominance inside the cyber domain. By doing so, China is aiming to subdue enemies in cyber space without battle.

A further observation to make is that a nation's fears over the cyber domain show a link to previous negative events in that nation's history. Billo (2004) states that Russia's fear is that it will become engaged in a cyber arms race with the United States that it cannot win, resembling the struggle faced during the Cold War. Similarly, US Secretary of Defense Leon Panetta (2011–2013) has expressed the United States' concerns over being the victim of a digital Pearl Harbor (United States Department of Defense, February 2013). Looking at this evidence, it can be argued that events of the past are shaping the direction of national cyber warfare doctrines today.

The amount of literature in this area is vast, but even a brief survey demonstrates that nations are concerned about cyber warfare. As an issue of national security, it must be noted that nations are unlikely to publicise the full truth of their approaches and authors may be restrained in what material they are permitted to publish. Further still, nations have an incentive to actively spread disinformation regarding their strategies, capabilities and actions to avoid giving potential adversaries a knowledge advantage. With these issues in mind, the task of identifying true approaches and activities of nation's will always remain a particularly challenging one for the research community.

4.9. *Conceptualising cyber warfare*

A final challenge to consider is that of conceptualising cyber warfare. While many of the previously discussed topics are quite specific in their scope, this topic is somewhat broad and attempts to present ways of thinking about cyber warfare. One such example of this is Tibbs (2013) presenting the conceptual idea that cyber warfare can be seen as a game, with anyone using an internet connected device being a player. Tibbs suggests that anyone can be a player in the cyber game, but that states wield the most power. To aid in visualising the cyber game, Tibbs presents a cyber game board, which shows the various positions a player can take. This is shown in Fig. 7.

One axis describes the type of power a player can exert, the other axis represents where in the cyber domain this power is exerted. For example, if coercive power is used upon the connection domain, this may result in physical attacks on cables to cause denial of service to another player in the game. On the opposite end of the scale, a player using cooperative power in the cognitive domain may be sharing knowledge and understanding. According to Tibbs, players

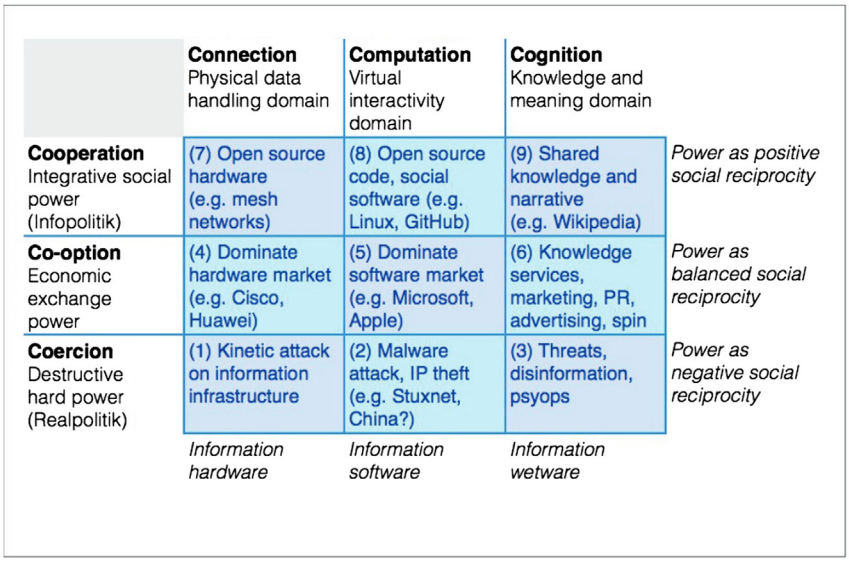

Fig. 7 – : Tibbs' Cyber game board (Tibbs, 2013).

are free to move around the game board, with the ultimate goal being to gain an advantage over other players. This is a novel view of conflict in the cyber domain and provides a well defined way to position various players and view their approaches.

While authors such as Tibbs attempt to present different ways of looking at the cyber domain, others such as Libicki (2012) have argued that cyber should not even be regarded as a domain. Libicki argues that traditional domains such as air, sea, land and space are natural, whilst cyber is a man made creation. Kuehl (2009) disagrees with this view, stating that the cyber domain can be seen as natural. In early warfare, the air existed but was not viewed as a domain of war simply because there was no way to enter it. When looking at cyber, the same argument can be made. The electromagnetic space has always existed, but we have only recently found suitable vessels for operating inside of it. The US Department of Defense also disagrees with Libicki, and asserts that there are five warfighting domains, which includes cyberspace (US Dept of Defence, 2013). Ultimately, the debate on whether cyberspace is or is not a warfighting domain is unlikely to be resolved by academia, and it can be argued that it should not be. Militaries are the experts of warfighting, and the decision to classify cyberspace as a warfighting domain or not should arguably be left to them.

Another view on cyber warfare is that its role as the future of war is being exaggerated beyond what is reasonable. Gartzke (2013) supports this view, stating that cyber warfare is only useful when it is used alongside traditional warfare. He compares cyber warfare to the use of artillery: While clearly useful, it alone cannot win wars and is just one tool of many that are needed to achieve meaningful gains. Applying this view to our definitions, Gartzke implies that while cyber warfare is useful, cyber war (a war fought only in the cyber domain) is not a useful endeavour since cyber attacks alone cannot win a war. Rid (2012) also supports this position, stating that cyber war has never and will never take place.

5. Conclusions and thoughts for the future

This paper has provided a survey of contemporary thought on the challenges presented by cyber warfare. It began by looking at existing definitions of cyber war and cyber warfare, and found two problems that needed resolving. Firstly, it was found that there is no widely accepted definition of either cyber war or cyber warfare. This is problematic since without an agreed definition, it is difficult to discuss the deeper issues or even recognise when cyber warfare is occurring. Secondly, we found that the terms cyber war and cyber warfare are often used interchangeably. We argued that this was also problematic, since the terms warfare and war have separate definitions. We addressed these problems by introducing the actor and intent definition model, which better defined both cyber warfare and cyber war.

We then identified nine research topics that present a challenge to the research community. These topics were examined, and views from the various authors in that field were analysed and contrasted.

While progress is being made to address these challenges, there are still significant gaps in research that need addressing, a number of which have been identified in this paper. The most significant conclusion to be made is that the majority of challenges presented by cyber warfare cannot be solved from the perspective of just one discipline. For example, attribution and cyber defence are certainly technical problems, but political, legal and social input is required to fully resolve these and other issues. Similarly, creating a set of laws for cyber warfare requires not just legal input, but technical and military input on what is feasible to enforce. With this in mind, it

must be concluded that a multi-disciplinary method is the best approach future research can adopt.

REFERENCES

Alford L. Cyber warfare: a new doctrine and taxonomy. US Air Force; April 2001. URL, http://www.crosstalkonline.org/storage/issue-archives/2001/200104/200104-Alford.pdf [accessed 25.05.14].

Alperovitch D. Towards establishment of cyberspace deterrence strategy. In: Cyber conflict (ICCC), 2011 3rd international conference on; 2011. p. 1–8.

Apps P. Analysis: in cyber era, militaries scramble for new skills. Reuters; February 2012. URL, http://www.reuters.com/article/2012/02/09/us-defence-cyber-idUSTRE8182HI20120209 [accessed 23.06.14].

Arimatsu L. A treaty for governing cyber-weapons: potential benefits and practical limitations. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–19.

Arquilla J, Ronfeldt D. Cyberwar is coming!. 1993. http://www.rand.org/pubs/reprints/RP223.html [accessed 12.11.14].

Billo C. Cyber warfare an analysis of the means and motivations of selected nation states. Dartmouth College; November 2004. URL, http://www.ists.dartmouth.edu/docs/cyberwarfare.pdf [accessed 10.04.14].

Boebert WE. A survey of challenges in attribution. In: Proceedings of a workshop on deterring CyberAttacks: informing strategies and developing options for U.S. policy; 2010. URL, http://cs.brown.edu/courses/csci1800/sources/lec12/Boebert.pdf.

Carr J. Inside cyber warfare. 2nd ed. O'Reilly Media Inc; 2012.

Caton J. Exploring the prudent limits of automated cyber attack. In: Cyber conflict (CyCon), 2013 5th international conference on; 2013. p. 1–16.

Clark D, Landau S. Untangling attribution. In: Proceedings of a workshop on deterring CyberAttacks: informing strategies and developing options for U.S. policy; 2010. p. 25–40.

Clarke RA, Knake R. Cyber war: the next threat to national security and what to do about it. Ecco; 2010. URL, http://www.harpercollins.com/browseinside/index.aspx?isbn13=9780061962233.

Cohen T. Obama: red line on syria is the world's, not his. CNN; September 2013. URL, http://edition.cnn.com/2013/09/04/politics/us-syria/?hpt=hp_t2 [accessed 15.06.14].

Colarik A, Janczewski L. Developing a grand strategy for cyber war. In: Information Assurance and Security (IAS), 2011 7th international conference on; 2011. p. 52–7. http://dx.doi.org/10.1109/ISIAS.2011.6122794.

Cornish P, Livingstone D, Clemente D, Yorke C. On cyber warfare. Chatham House; November 2012. URL, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/r1110_cyberwarfare.pdf [accessed 18.04.14].

Customary international Humanitarian Law. Rule 65: Perfidy, The Red Cross. 2005. URL, http://www.icrc.org/customary-ihl/eng/docs/v1_cha_chapter18_rule65 [accessed 15.04.14].

Denning DE. Information warfare and security. New York: ACM Press; 1999.

Denning DE. Reflections on cyberweapons controls. Comput Secur J 2000;16(4):43–53. URL, http://www.rand.org/pubs/external_publications/EP51077.html.

Dever J, Dever J. Cyberwarfare: attribution, preemption, and national self defense. J Law Cyber Warf 2013. Summer, 2(1).

Dipert RR. The ethics of cyberwarfare. J Mil Ethics 2010;9(4):384–410. http://dx.doi.org/10.1080/15027570.2010.536404. arXiv: http://www.tandfonline.com/doi/pdf/10.1080/15027570.2010.536404. URL http://www.tandfonline.com/doi/abs/10.1080/15027570.2010.536404.

Dogrul M, Aslan A, Celik E. Developing an international cooperation on cyber defense and deterrence against cyber terrorism. In: Cyber conflict (ICCC), 2011 3rd international conference on; 2011. p. 1–15.

Fanelli R, Conti G. A methodology for cyber operations targeting and control of collateral damage in the context of lawful armed conflict. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–13.

FBI. Terrorism definition. 2014. URL, http://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition [accessed 25.05.14].

Fernández Vázquez D, Pastor Acosta O, Brown S, Reid E, Spirito C. Conceptual framework for cyber defense information sharing within trust relationships. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–17.

Foltz AC. Stuxnet, schmitt analysis, and the cyber "use of force" debate. Jt Force Q 2012;67:40–9.

Friesen T. Resolving tomorrow's conflicts today: how new developments within the U.N. security council can be used to combat cyberwarfare. In: Naval law review; 2009.

Fuller B. Federal intrusion detection, cyber early warning and the federal response. SANS Institute; 2003. URL, http://www.sans.org/reading_room/whitepapers/warfare/federal-intrusion-detection-cyber-early-warning-federal-response_1095 [accessed 14.04.14].

Gartzke E. The myth of cyberwar: bringing war in cyberspace back down to earth. Int Secur 2013;38(2):41–73. http://dx.doi.org/10.1162/ISEC_a_00136. http://dx.doi.org/10.1162/ISEC_a_00136.

Golling M, Stelte B. Requirements for a future ews – cyber defence in the internet of the future. In: Cyber conflict (ICCC), 2011 3rd international conference on; 2011. p. 1–16.

Hare F. The significance of attribution to cyberspace coercion: a political perspective. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–15.

Hunker J, Hutchinson B, Margulies J. Role and challenges for sufficient cyber-attack attribution. January 2008. URL, http://www.thei3p.org/docs/publications/whitepaper-attribution.pdf [accessed 16.07.14].

Jesson M, Lacey. Doing your literature review: traditional and systematic techniques. SAGE Publications Ltd; 2011.

Kalutarage H, Shaikh S, Zhou Q, James A. Sensing for suspicion at scale: a bayesian approach for cyber conflict attribution and reasoning. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–19.

Kitchenham B, Brereton P, Li Z, Budgen D, Burn A. Repeatability of systematic literature reviews. In: Evaluation assessment in software engineering (EASE 2011), 15th annual conference on; 2011. p. 46–55. http://dx.doi.org/10.1049/ic.2011.0006.

Koh HH. International law in cyberspace. 2012. URL, http://www.state.gov/s/l/releases/remarks/197924.htm [accessed 09.06.14].

Kopp C. Information warfare: a fundamental paradigm of infowar, systems: enterprise computing monthly. 2000. p. 46–55.

Krever M. Fmr. cia official: cyber war more sinister than nuclear age. CNN; February 2013. URL, http://amanpour.blogs.cnn.com/2013/02/19/fmr-cia-official-cyber-war-more-sinister-than-nuclear-age/ [accessed 16.05.14].

Kuehl DT. Cyberpower and national security, Potomac books and national defense university. In: Ch. from cyberspace to cyberpower: defining the problem; 2009. p. 24–42.

Kushner D. The real story of stuxnet. IEEE Spectrum; Februrary 2013. URL, http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet [accessed 02.06.14].

Laprise J. Cyber-warfare seen through a mariner's spyglass. Technol Soc Mag IEEE 2006;25(3):26–33. http://dx.doi.org/10.1109/MTAS.2006.1700019.

Libicki MC. Cyberdeterrence and cyberwar. RAND Corporation; 2009. URL, http://www.rand.org/pubs/monographs/MG877.html.
Libicki MC. Cyberspace is not a warfighting domain. I/S: J Law Policy Inf Soc 2012;8(2):325–40. URL, http://www.rand.org/pubs/external_publications/EP51077.html.
Libicki M. What is information warfare?. National Defense University; August 1995. URL, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA367662 [accessed 26.05.14].
Liles S, Rogers M, Dietz J, Larson D. Applying traditional military principles to cyber warfare. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–12.
Lin P, Allhoff F, Rowe NC. War 2.0: cyberweapons and ethics. Commun. ACM 2012;55(3):24–6. http://dx.doi.org/10.1145/2093548.2093558. http://doi.acm.org/10.1145/2093548.2093558.
Lonsdale D. The nature of war in the information age: Clausewitzian future. Routledge; 2004.
Marcus J. Are we really facing cyberwar?. BBC News; March 2013. URL, http://www.bbc.co.uk/news/technology-21653361 [accessed 18.05.14].
NATO. The tallinn manual on the international law applicable to cyber warfare. March 2013. URL, www.ccdcoe.org/249.html [accessed 22.05.14].
Nicholson A, Webber S, Dyer S, Patel T, Janicke H. Scada security in the light of cyber-warfare. Comput Secur 2012;31(4):418–36. http://dx.doi.org/10.1016/j.cose.2012.02.009. URL, http://www.sciencedirect.com/science/article/pii/S0167404812000429.
Nicholson A, Janicke H, Watson T. An initial investigation into attribution in scada systems. In: ICS & SCADA cyber security research, 1st international symposium for; 2013.
O'Connell ME. Cyber security without cyber war. J Confl Secur Law 2012;17(2):187–209. URL, http://jcsl.oxfordjournals.org/content/17/2/187.full.pdf?keytype=ref%2520&ijkey=T6J6KDRCRcHM4Ao.
Oxford English dictionary. Oxford University Press; 2013.
Paret P, Craig G, Gilbert F, editors. Makers of modern strategy from Machiavelli to the nuclear age. Princeton University Press; 1986.
Parks R, Duggan D. Principles of cyberwarfare, security privacy. IEEE 2011;9(5):30–5. http://dx.doi.org/10.1109/MSP.2011.138.
Powell R. Nuclear deterrence theory: the search for credibility. Cambridge University Press; 1990.
Protocol I of the Geneva conventions. Red Cross; 1977. URL, http://www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 [accessed 23.05.14].
Rauscher K, Korotkov A. Working towards rules for governing cyber conflict. January 2011. URL, http://www.ewi.info/working-towards-rules-governing-cyber-conflict.
Rid T. Cyber war will not take place. J Strateg Stud 2012;35(1):5–32.
Rowe N. The ethics of cyberweapons in warfare. Int J Cyber Eth 2010;1(1):20–31.
Saydjari OS. Cyber defense: art to science. Commun ACM 2004;47(3):52–7. http://dx.doi.org/10.1145/971617.971645. URL, http://doi.acm.org/10.1145/971617.971645.
Saydjari O. Structuring for strategic cyber defense: a cyber manhattan project blueprint. In: Computer security applications conference, 2008. ACSAC 2008. Annual; 2008. p. 3–10. http://dx.doi.org/10.1109/ACSAC.2008.53.
Schmitt M. Attack as a term of art in international law: the cyber operations context. In: 4th international conference on cyber Con; 2012.
Schmitt M. Classification of cyber conflict. J Confl Secur Law 2012b;17(2):245–60.
Schmitt M. Computer network attack and the use of force in international law: thoughts on a normative framework. In: Essays on law and war at the fault lines. T. M. C. Asser Press; 2012c. p. 3–48. http://dx.doi.org/10.1007/978-90-6704-740-1_1.
Schmitt M. International law in cyberspace: the koh speech and tallinn manual juxtaposed. Harv Int Law J 2012d;54. Online. URL, http://www.harvardilj.org/2012/12/online-articles-online_54_schmitt/.
Schneier B. Has U.S started an internet war?. CNN; June 2013. URL, http://edition.cnn.com/2013/06/18/opinion/schneier-cyberwar-policy [accessed 27.05.14].
Sharma A, Gandhi R, Mahoney W, Sousan W, Zhu Q. Building a social dimensional threat model from current and historic events of cyber attacks. In: Social computing (SocialCom), 2010 IEEE second international conference on; 2010. p. 981–6. http://dx.doi.org/10.1109/SocialCom.2010.145.
Sterner E. Retaliatory deterrence in cyberspace. Strateg Stud Q 2011:62–80. URL, http://www.marshall.org/pdf/materials/933.pdf.
Taddeo M. An analysis for a just cyber warfare. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–10.
Thomas TL. Cyberpower and national security, Potomac books and national defense university. In: Ch. Nation-state cyber strategies: examples from China and Russia; 2009. p. 465–90.
Tibbs H. The global cyber game. 2013. URL, http://www.da.mod.uk/publications/library/technology/20130508-Cyber_report_final_U.pdf [accessed 10.06.14].
Traynor I. Russia denounces ukraine 'terrorists' and west over yanukovich ousting. BBC News; February 2014. URL, http://www.theguardian.com/world/2014/feb/24/russia-ukraine-west-yanukovich [accessed 25.05.14].
Tyugu E. Command and control of cyber weapons. In: Cyber conflict (CYCON), 2012 4th international conference on; 2012. p. 1–11.
Tzu Sun. The art of war. Shambhala Publications; 2005.
Uk 'complacent' over military cyber-attack risk, mps warn. BBC News; January 2013. URL, http://www.bbc.co.uk/news/uk-politics-20952374 [accessed 22.05.14].
Ukraine says donetsk 'anti-terror operation' under way. BBC News; April 2014. URL, http://www.bbc.com/news/world-europe-27035196 [accessed 25.05.14].
United States Department of Defense. Panetta warns cyber threat growing quickly. February 2013. URL, http://www.defense.gov/news/newsarticle.aspx?id=119214 [accessed 10.06.14].
United States Department of Defense. Department of defense strategy for operating in cyberspace. July 2011. URL, http://www.defense.gov/news/d20110714cyber.pdf [accessed 11.05.14].
US Dept of Defence. Law of armed conflict deskbook. 2012. URL, http://www.loc.gov/rr/frd/Military_Law/pdf/LOAC-Deskbook-2012.pdf [accessed 05.07.14].
US Dept of Defence. Air-sea battle. May 2013. URL, http://www.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf [accessed 05.06.14].
U.S. Joint Chiefs of Staff. Information operations. November 2012. URL, http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf.
Vlahos KB. Special report: the cyberwar threat from north korea. Fox News; February 2014. URL, http://www.foxnews.com/tech/2014/02/14/cyberwar-experts-question-north-korea-cyber-capabilities/ [accessed 26.05.14].
War in the fifth domain. The Economist; July 2010. URL, http://www.economist.com/node/16478792 [accessed 10.05.14].
Watts S. Proposal for cyber war rules of engagement. BBC News; February 2011. URL, http://news.bbc.co.uk/2/hi/programmes/newsnight/9386445.stm [accessed 23.05.14].
Wheeler D, Larsen G. Techniques for cyber attack attribution. October 2003. URL, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA468859 [accessed 23.07.13].
Wilking R. Expert: US in cyberwar arms race with China, Russia. NBC News; February 2013. URL, http://investigations.nbcnews.com/_news/2013/02/20/17022378-expert-us-in-cyberwar-arms-race-with-china-russia [accessed 25.05.14].

Wohlin C, Prikladnicki R. Systematic literature reviews in software engineering. Inf Softw Technol 2013;55(6):919–20. http://dx.doi.org/10.1016/j.infsof.2013.02.002. URL, http://www.sciencedirect.com/science/article/pii/S0950584913000359.

Michael Robinson is a PhD student at De Montfort University (UK) with an interest in cyber warfare research. He has a multi-disciplinary background with Batchelor degrees in both computer science and international relations. He received his Masters degree in computer security from De Montfort University in 2012.

Dr. Helge Janicke is a Reader in Computer Science at De Montfort University, Leicester (UK). He is heading the Software Technology Research Laboratory and is leading research on Cyber Security. His research interests are in particular the Cyber Security of Industrial Control Systems, Access Control and Policy-based System Management.

Dr. Kevin Jones is the Research Team Lead for Airbus Group Innovations Cyber Operations. He is active in the cyber security research community and holds a number of patents within the domain. He has many years' experience in consultancy to aid organisations in achieving accreditation to ISO27001 Standard on Information Security Management and lecturing in cyber security. Kevin joined Airbus in 2011 where he has researched risk assessments, security architectures, and cyber operations in numerous domains including, ICS/SCADA systems and Critical National Infrastructure (CNI). He is a Member of BCS, IEEE and ISC2 and is accredited as a Certified Information Systems Security Professional (CISSP) and ISO27001 Lead Auditor.