Controlling Uncertainty with Proactive Cyber Defense: A Clausewitzian Perspective

Sampsa Rauti

University of Turku, 20014 Turku, Finland
sjprau@utu.fi

Abstract. This study argues that the fundamental tenets Carl von Clausewitz presented about warfare in his influential book *On War* can be applied to defensive cyberwar. This will help in forming a new multidisciplinary perspective on the topic, which can benefit policy makers, political and military scientists and cyber security specialists alike. Moreover, by applying Clausewitz's principles of defensive warfare and his concepts of uncertainty and friction to cyberdefense, we outline a conceptual framework for resilient and proactive cyberdefense.

1 Introduction

With the ongoing digitalization of society, cyberwar is being discussed everywhere. The term has gained popularity after the cyberattacks in Estonia in 2007 [22]. In the academic literature, political scientists, military-academic scholars, and technical cyber security experts have studied the topic actively. The debate has often circled around how to define cyberwar or whether cyberwar exists in the first place.

Carl von Clausewitz's extensive work *On war* is commonly seen as the most essential book on warfare in the Western world [15]. Therefore, it is not that surprising several scholars have applied Clausewitz's principles to cyberwar, although the book was written back in 1832 [13, 18, 6, 32]. Many argue that cyberwar is coming [7, 30], while other academics are skeptical or deny the whole existence of cyberwar [32, 14]. This discussion seems to mainly derive from the lack of a commonly agreed definition for cyberwar and cyberattack [26].

Regardless of the exact definition of cyberwar, cyberconflict and cyberattacks do exist and they have real implications for society and the physical world. We argue that Clausewitz can provide a useful framework for analyzing the incidents in cyberspace, cyberconflicts and cyberattacks. It is an interesting theoretical lens through which cyberwar can be discussed and understood from a new perspective. Using Clausewitz's principles, we can also bridge the conceptual gap between disciplines of cyber security and political science and give both sides a new conceptual tool to examine cyber attacks and cyber defense.

As the title suggests, this study concentrates on defensive cyberwar. It is well known that Clausewitz sees defense as the stronger form of waging

war compared to offense [8, p. 358]. On the other hand, in the cyberspace the attacking side is usually thought to be stronger. While it may be true that the attacker has an upper hand in cyberspace in several situations, it is interesting to see how Clausewitz's principles can be used to analyze and strengthen cyber defenses.
The primary contribution of this study is to link Clausewitz's conceptual description of defensive war to the technical concepts and means of realizing cyber defenses. Specifically, we argue Clausewitz's framework can be linked to many proactive cyberdefenses that increase uncertainty for the attacker and employ deception technology to protect computer systems. It could be interesting for policy makers, political scientists, technical cyber security experts alike to learn what Clausewitz can teach us about the subject. Military scientists can also benefit from understanding both political and technical side of cyberwar.
The rest of the paper is organized as follows. Section 2 discusses the main principles presented by Clausewitz and the applicability of *On War* in cyberspace. Section 3 analyzes how Clausewitz's principles can be applied to implement proactive cyber defenses and how these ideas can be translated into technical concepts in order to better thwart cyberattacks. Section 4 contains the discussion and Section 5 presents some concluding remarks.

2 Background

2.1 The main ideas of the Clausewitzian framework

Clausewitz's most well-known aphorism is probably the famous statement that war is "a continuation of political intercourse, carried on with other means." [8, p. 87] It is worth noting, however, that the German word *Politik* Clausewitz originally used is not only restricted to state affairs [18]. In *On War*, the word is not only used to refer to politics but also to *policy*. A policy can be briefly defined as a set ideas and decisions by a state or group to pursue an objective. An important thing to note in the context of cyberspace is that as Clausewitz is not a state-centrist (although he is often mistakenly interpreted as one). Therefore, the Clausewitzian framework also allows the actors other than states, such as hacktivist groups, to participate in cyber war. For the same reason it is not a problem for the framework that the states cannot fully control what happens in cyberspace.
Clausewitz also states that the war is an act where the enemy is rendered powerless and forced to comply with the attacker's will [8, p. 75]. However, in reality, war does not always lead to the destruction of the enemy. Forcing the enemy the do one's will can take many forms, and warfare can also include methods such as cyber attacks.
For success in war, Clausewitz stresses the importance of a clear objective (defined by a policy or politics). Creative and talented army that can counter the enemy and handle the unpredictability of the war is also a necessity. Moreover, passion of the people is also a vital component of success. It is easy to see these elements are also important in cyberwar. A

cyber operation cannot even begin without a clear objective, and creativity and talent are necessary in order to implement and use cyberweapons or defense mechanisms. Passion of the people is also an interesting point in the context of cyberwar – in modern digitalized society the cyberspace is open for any passionate individual to participate in cyber operations.

A very important concept in cyberspace is *friction*. It refers to the unpredictability and unforeseen occurrences in war, which inexorably make the real war different from a plan on paper [8, p. 119]. In cyberspace, friction might include bad network connections, unexpected collateral effects and programming mistakes made by humans. However, what makes friction especially interesting in cyberspace in our opinion is the constantly changing structure of and the complexity of cyberspace. Also, what Clausewitz says about friction and unpredictability in form of unreliable information [8, p. 117] is especially true in cyberspace. This is because unlike the physical world, one does not really have anything tangible as a proof of the authenticity of information. Instead, one only receives network messages and information in digital form, the contents of which can often be forged quite easily.

It follows from the significance of friction that it is very important for a good general to understand the uncertainty that friction causes, and to be able to see through this "fog of war" as well as possible. An essential ability when aiming to disperse the fog of uncertainty is something Clausewitz calls *coup d'oeil*. He describes this as "an intellect that, even in the darkest hours, retains some glimmerings of the inner light which leads to truth" [8, p. 102]. In other words, the commander's coup d'oeil is intuition, the ability to recognize truth quickly. In more modern terms, the commander is quickly able to reach a state of accurate *situational awareness*, a conception that "the mind would ordinarily miss or would perceive only after long study and reflection." [8, p. 102] Naturally, a good situational awareness and the ability to make quick decisions without hesitation (determination) are essential in fast-paced cyberwar. Therefore, in our view, coup d'oeil and determination should also be taken into account when applying *On War* in cyberspace. Unfortunately, nearly all writings discussing how to apply Clausewitz's framework in the age of cyberwar have failed to do so [18, 32].

Finally, Clausewitz divides warfare into offensive and defensive forms. One of the main arguments Clausewitz makes is that defense is an inherently stronger form of war [8, p. 102]. Many theorists such as Farwell [12] have claimed this principle can not be applied to cyberwar, because in cyberspace, the attacker has an advantage over the defender. As we will discuss later, and as also noted by [18], this assumption is not necessarily true. Clausewitz goes on to explain how the familiar *terrain* usually gives the benefit to the defender.

We strongly believe these concepts, summarized in Table 1, can also be applied in cyberspace and used to bridge the conceptual gap between practitioners of political and military sciences and cyber security specialists. Defensive warfare and applying Clausewitz's framework to cyber defense is the topic we will turn to next.

Table 1. Clausewitzian concepts and their counterparts in cyberspace.

Concept	**Meaning in cyberspace**
Friction	Intrinsic uncertainty of cyberspace and potential countermeasures introduced by the defender
Terrain	Cyberterrain – structure of a targeted network or a computer system and its interfaces, can be modified to increase friction
Coup d'oeil	Situational awareness based on the gathered data
Creative army	Creatively devising defense mechanisms
Passionate people	Anyone with an access to cyberspace may take part in cyberconflicts

2.2 Can Clausewitzian principles be applied to cyberspace?

It may be seem weird or even absurd to apply principles devised in 1800s to modern cyberattacks. However, as we will see, many high level principles and maxims presented in *On War* still remain valid today. Regardless, it is worth taking a brief look at why we agree with several other authors (such as [30] and [18]) that most Clausewitzian principles have retained their validity, and can be used as a useful lens through which cyberwarfare can be analyzed and understood.

In the debate on cyberwar, Thomas Rid [32] has been one of the most vocal advocates of the view that "cyberwar is not coming". Rid argues that according to Clausewitzian principles, lethal violence is a necessary element in warfare, and cyberwar completely lacks this important characteristic. While violence undeniably does play a role in the Clausewitzian framework, we also have to take into account how the concepts change over time [19]. In fact, Clausewitz himself repeatedly notes that war is a true chameleon that changes its nature regularly [8, p. 89].

The nature of war has indeed changed – technology plays a bigger role in war than before and information is becoming a more and more important resource in today's digitalized world. Violence may not be such an essential element in all areas of warfare anymore, or at the very least, violence does not need to be lethal or physical in cyber warfare. If one only constrains violence to the physical world, its manifestations in cyberspace, used to achieve the same objectives, will be disregarded [4]. That having been said, some cyberattacks, such as the Stuxnet worm targeting a uranium enrichment facility in Iran, do have the ability to cause physical harm. This threat will only grow more prominent as cyberspace continues to become increasingly intertwined with the physical world. Clausewitz also notes that war is an act to compel our enemy to do our will [8, p. 75]. Physical violence, however, is only an instrument to achieve this objective. The goal can often be accomplished by using alternative methods in cyberspace. Clausewitz states: "When we speak of destroying the enemy's forces we must emphasize that nothing obliges us to limit this idea to physical forces: the moral element must also be considered." [8, p. 97]

Thomas Rid and many other authors who rebut cyberwar also seem to discuss "pure" cyberwar that would be fought only, or at least primarily, in cyberspace. This kind of cyberwar is indeed unlikely to take place in the foreseeable future. The possible dangers of cyberwar are often greatly exaggerated and cyberwar is currently not a "one strike and you are out" type of threat like some doomsday scenarios seem to imply. However, cyber warfare can still be seen as one dimension of war [5]. There does not need to be pure cyberwar without traditional dimensions of warfare and for now, this would be an unrealistic assumption.

Of course, it would probably be correct to argue that the four first dimensions of warfare – land, sea, air and space – can often be used much more effectively to quickly achieve strategic objectives compared to the fifth dimension, cyberspace. However, not all parts of warfare are about using extreme force and Clausewitz was well aware of this fact when introducing the concept of *limited war* [8, p. 612]. In fact, Clausewitz only uses "total war" as a theoretical, ideal type of war that does not occur in practice. Indeed, in today's world, there are many conflicts where the political objective is not to conquer enemy territory or overthrow government, but the end goal can be something much smaller, and therefore, the applied methods to achieve the objective also do not need to be lethal or physically destructive. Modern hybrid warfare [1, 27] takes place in a grey zone between war and peace, and also employs many unconventional means to reach the desired objective. In the Clausewitzian framework, the political objective explains the war, and the means used to achieve it are less important.

Moreover, while the discussion about the concept of cyberwar is still definitely necessary, the semantic rigor and pedantry associated with many theories about cyberwar can sometimes prevent us from concentrating on what is really happening in reality [4, 21]. The term cyberwar is already widely used and acknowledged as the fifth dimension of warfare, and most importantly, it is treated as a hostile act that can be countered with the use of military force. For instance, in the "International Strategy for Cyberspace", published in 2011, the White House states that military force can be used in response to a cyberattack [34].

Finally, Clausewitz intended the write a book that would resist the effects of time. The reason the Clausewitzian framework still remains valid to a great extent today is that Clausewitz's main principles are not dependent on the current technology that is employed in waging war. Therefore, the timeless framework is useful also in cyberspace. Nevertheless, it is worth noting that it would be an anachronism to directly claim Clausewitz had something to say about cyberwar. Although Clausewitz did not predict the age of cyberwar, he created a framework that can be successfully connected to the concepts of modern cyber warfare.

3 A Clausewitzian perspective to cyberdefense

3.1 Is defense weaker than offense in cyberspace?

Considering the nature of interconnected cyberspace, one can easily think that offense is inherently stronger than defense. In cyberspace, where

data can travel from the other side of the world instantly and all the connected devices can connect to other devices immediately, it is easy to think launching successful cyberattacks is easy and lightning fast. However, in order to launch a cyberattack and infiltrate an enemy system successfully, one has to know what kind system the enemy possesses and what are the potential vulnerabilities the system has. Gathering intelligence on the enemy's system, discovering previously unknown vulnerabilities and possibly creating new cyber weapons – that is, writing custom malware – takes resources, time and money.

If we assume that systems are regularly updated and patched – like they should be in any critical infrastructure that is likely to be at the receiving end of cyber attacks – the same vulnerabilities can not be continuously exploited over a long period of time. Finding new vulnerabilities again takes more time. Although a hundreds of thousands of unique pieces of malware are manufactured every day [3] and many of them only consist of few hundred lines of code, finding exploitable vulnerabilities still remains a challenge for the attacker. The oft-repeated argument that cyber attacks consume no resources is therefore not completely correct.

Moreover, even when the attacker has succeeded to infiltrate the system, this can still be detected and the system can be defended, by using intrusion detection systems or proactive cyber defense mechanisms, for instance. It is important to note that cyber defenses are often multilayered, which also strengthens defense. Also, when an attacker has infiltrated our system, we can get lots of useful information about enemy's technologies and objectives if we have an appropriate intrusion detection system in place. Attackers are always in the danger of revealing critical information about themselves.

Many existing and well-known exploits also demonstrate that a successful attack often either takes a lot of work or is dependent on infecting systems with very poor cyber security. Take the Stuxnet worm we mentioned before, for example. The Stuxnet source code made use of four previously unknown zero-day vulnerabilities [11]. It is quite clear the malware was created by professionals who had a good understanding of how cyber defenses such as anti-virus technologies work, as well as information about yet unknown vulnerabilities. While Stuxnet is an extreme example, it demonstrates that an advanced attack requires lots of work and carefully gathered knowledge about the target system.

Another interesting example is the Mirai malware from 2016. Mirai turns infected network devices running the Linux operating system into remotely controlled bots [17]. These bots then form a botnet that can be used to launch large-scale distributed denial of service (DDoS) attacks, which can cause disturbances in web services or even cause services to go offline. Mirai infected tens of thousands of Internet of Things (IoT) devices easily, but only because their security was so poor that the default passwords had not been changed. In this case, cyber defense was just poor, not really intrinsically weaker than offense. Unfortunately, large numbers of IoT devices still have poor security [10], which gives advantage to cyber attackers in many cases.

Of course, sometimes cyber attacks do overpower defenses. For instance, large DDoS attacks are often difficult to counter immediately. Also, in

the cases where the adversary has planted a backdoor[1] or a logical bomb[2] in the system beforehand, the attacker has the initial advantage. Even in these cases, however, the attacker has done some work beforehand, by gathering information and infecting vulnerable machines. Also, Clausewitz actually states that the attacker often has an initial advantage, but the defender becomes stronger when the battle drags on [8, p. 624].
It is difficult to conclusively evaluate whether defense is stronger form of warfare in cyberspace. However, because in many cases only successful cyberattacks are noticed and get media coverage, and failed attacks are not always even detected or they are kept secret, it would seem the strength of cyberattacks is often overestimated compared to defenses. As Jacobsen states, this stance can then easily become a self-fulfilling prophecy [18]. Clausewitz's framework can help us to see things differently and provide interesting insights on how to better take defensive warfare into account.

3.2 Taking control of uncertainty and friction

Based on the discussion above, it seems Clausewitz's framework can be applied to cyber defense, but how exactly can we derive benefit from it? As we have seen before, Clausewitz maintains that uncertainty is a central component in war: "War is the realm of uncertainty; three quarters of the factors on which action in war is based are wrapped in a fog of greater or lesser uncertainty." [8, p. 101]. Strongly associated with this uncertainty is the concept of friction. Friction causes a difference between how things are expected happen on paper and the actual way they happen due to unexpected distractions [8, p. 119]. Unexpected events cause friction that sets the initial plan off course. In cyberspace, too, there are many things that are beyond our control, such as mistakes made by humans and unexpected collateral effects of cyber attacks, for instance. However, it is interesting to note that in cyberspace we can also effectively attempt to use the friction to our advantage by causing asymmetry between the friction we encounter and the friction the enemy experiences. Clausewitz notes that the defender has the advantage of familiar terrain in the battle [8, p. 269,361]. This home-field advantage is even greater in cyberspace because the "cyberterrain" can be shaped according to the defenders needs much more easily than in the physical world. This is definitely something the defender can proactively take advantage of even before a cyberattack takes place. As Clausewitz observes, the terrain can act "as an obstacle to the approach, as an impediment to visibility, and as cover from fire", making the attackers job more difficult [8, p. 348].
In what follows, we will discuss methods to take control of uncertainty and friction, both by making the enemy encounter more uncertainty and by attempting to provide our own cyber army with the necessary tools to see through the thick fog. Here, we will mainly limit our discussion to

[1] A backdoor is a method that allows a system security mechanism to be bypassed secretly to access computer system and its data.

[2] A logic bomb is a piece of harmful code, inserted in a computer system. When certain conditions are met, the code will execute predefined malicious functionality.

technical methods.

Make the cyber terrain unpredictable by diversity. Friction can be introduced and cyberterrain the adversary has to navigate can be made more uncertain by introducing software diversity in the target system under attack. Malicious attackers and programs benefit from the fact that computers use a relatively small group of different operating system versions. In other words, software monoculture prevails and an attacker can plan cyber attacks that use well-known facts about the target system. For instance, a malicious program can use a well-know operating system interface in the system to reach its goals (for example, to open and edit files with sensitive information). However, if the interfaces malware wants to use and interact with were uniquely diversified in each system, the malware would have much more trouble attempting to reach its goals [9]. It would no longer know the "language" of the system under attack. This would probably render the piece of malware useless for quite some time. This way, asymmetric friction can be created through increased resilience, and the system can be defended effectively without disturbances in its operation. There are methods to create diverse software systems automatically without human intervention [20, 24].

Dynamically changing cyberterrain. As new attacks are launched, the advantage between attackers and defenders seems to continuously keep shifting. To use the friction to defenders advantage in an attempt to stop this never-ending cycle, the paradigm of moving target defense (MTD) can be employed [16]. This defense mechanism creates a dynamic and constantly changing attack surface implemented across several system dimensions. As stated by Clausewitz, in the fast-paced war, one reason the gathered intelligence is unreliable is because it is so transient [8, p. 117]. When a report arrives, the situation has already changed.
MTD makes the shape of cyber terrain transient, which increases uncertainty for malicious adversaries and makes attacking the target much more difficult. After all, it is quite a challenge to attack something you cannot understand and see clearly. MTD can be applied to wide range of attacks surfaces in computer networks and systems. One example is to have a set of constantly evolving interfaces in the system. Unknown interfaces that constantly change are difficult targets for a malicious program or attacker. MTD can also be implemented on network level for example by constantly changing the IP addresses of certain targets.

Cyber Deception. Deception is one obvious way to expose the attacker to more friction and uncertainty. While Clausewitz does not seem to believe in deception and surprise on strategical level, he does suggest deceiving the enemy can be a very useful tactical maneuver when when conditions are favorable [8, p. 198]. Even though surprise is not the key element in success of the war, it can be a useful tactical device. In cyberspace, deception is easier than in the real battlefield, because cyberspace is made of bits and bytes that can be changed and forged quite easily, at least in our own territory we are defending. Moreover, because the enemy often appears in the form of a malicious program rather than

a living human, it is often easy to introduce uncertainty and friction. An intelligent hacker is naturally more difficult to fool for long periods of time.
How can an enemy be deceived in cyberspace? Different deception technologies can be used to provide an attacker with fake targets that look valuable [2, 9]. In terms of technical solutions, this can be anything from network with several honeypots machines (computers with data that appears to be valuable and interesting) to planting simple fake files in a system. Also the important system interfaces we mentioned previously could be forged in this manner. When someone interacts with these fake resources, we immediately know there is an attacker in the system, because no legitimate process or user should access these resources [35]. This is especially convenient for detecting previously unknown malware. Several fake targets will considerably slow down the attacker and the enemy is more likely to gather false intelligence.

Gathering intelligence. Honeypots and other fake resources are there not only for deception. They are also great at gathering intelligence about the enemy and their potential objectives [29]. With monitoring software, such as intrusion detection systems and honeypots, we can record information on what is going on in the network and in a specific system. For example, network packets arriving to and leaving from our local network and system calls issued in our systems can be recorded for further analysis [23]. According to Clausewitz, intelligence gathered in war is mostly untrustworthy and false, because fear has an effect of multiplying lies and inaccuracies [8, p. 117]. Automatically collected information does not have this weakness.
However, on a high level it is necessary to combine conflicting information from many sources, check credible external sources for worldwide cyber threat information, and also put together intelligence from other disciplines (human intelligence, geospatial intelligence) to get a comprehensive grasp of the current situation. The difficulty of recognizing the important pieces of information that should be prioritized constitutes one of the most serious sources of friction in war, because things often appear entirely different from what one has expected. Therefore, we need mechanisms to dig out the truth from the data we have gathered.

Coup d'oeil in cyberspace. Coup d'oeil, as we discussed previously, is a great general's intuitive grasp of what is going on in the battlefield. The process of quickly perceiving what is happening in the strategically significant locations in cyberspace and making a rapid and accurate decision can be made easier by making use of artificial intelligence (AI) that is able to provide the commander with appropriate situational awareness. This kind of tool could help the commanders to do better and improve the ability to use their coup d'oeil.
The process would still be human-centered – after all, with Clausewitz's principles, it is difficult to imagine an AI waging war independently – it would only provide a device to see through the fog and avoid the friction more effectively by providing necessary information for fast decisions. An advanced AI system can also have the ability to learn, and ultimately use

Table 2. Summary of proactive defenses.

Proactive defense	**Example**
Increase uncertainty by diversity	Diversifying system interfaces
Changing cyberterrain	Moving target defense
Cyber deception	Planting honeypots in a network
Gathering intelligence	Logging the adversary's activities
Coup d'oeil in cyberspace	Using AI to form situational awareness from the gathered data
Offensive defense	Giving fake data to the attacker

an extensive corpus of battle experience and knowledge to augment the commander's capability to weight different options and make decisions based on solid evidence and the underlying political objective.

Offensive defense Clausewitz maintains that even when war is defensive, it still often contains offensive components [8, p. 357]. Indeed, above we have already discussed methods that can be used to annoy the attacker and disrupt enemy operations. We can also annoy the attackers by feeding them false replies and information [31], while at the same monitoring how they react to this. This can also help us to get even more information on attacker's methods and objectives. Attribution – the process of tracking and identifying the perpetrator behind the attack – is also an important part of offensive cyber defense [25]. After all, if we do not know who the attacker is, we cannot strike back.

The proactive defenses are summarized in Table 2.

4 Discussion

In this study, we have suggested Carl von Clausewitz's principles of defensive warfare can be useful in conceptualizing and designing resilient methods for cyberdefense. Software diversification and moving target defense increase resilience of the defender's systems and at the same time, create uncertainty and friction for the enemy. Cyberterrain can further be modified with fake targets that annoy and stall the enemy, while also gathering intelligence. Finally, with an AI-enhanced coup d'oeil, talented commanders can assess the collected information and make the correct and quick decisions under stress and continuous information overload.
When the defender succeeds in adding enough uncertainty for the enemy, the situation can also be compared to the difficulties of executing a night attack described by Clausewitz. The attacker should effectively attack in the darkness and know the complete layout of enemy's defenses, while keeping its own disposition secret from the enemy for as long as possible [8, p. 273]. At the same time, the defender can see the familiar cyber terrain clearly and keep learning more about the enemy, while also preparing for a potential counterattack.

As cyberspace keeps getting increasingly intertwined with the physical world and critical infrastructure of society, significance of defending systems from cyber threats also keeps growing [28, 36]. Billions of networked IoT devices with poor security are a reminder of the fact that cyber security has not yet been taken as seriously as it should. This paper has presented a conceptual framework inspired by Clausewitz's ideas of defensive warfare and taking advantage of emerging proactive cyber defense mechanisms. Naturally, this is not to say we should not keep using more traditional security measures such as anti-virus software, encryption, whitelisting and strong authentication mechanisms. In the face of advanced persistent threats and zero-day exploits, however, we also need novel defenses that change the cyber terrain to our advantage and take control of uncertainty. Therefore, these defenses are not mutually exclusive. Indeed, a multilayered approach to defense fits well to today's complex cyber security landscape, where no single countermeasure is totally effective against every threat or exploit. Clausewitz writes about how important it is for a defender to have several fortresses that attract the attention of the enemy but are resilient enough to withstand attacks [8, p. 372].

It is also interesting to note that while our discussion of cyber defenses has mainly focused on technical considerations, Clausewitz also emphasizes a creative army and passion of the people as important factors in successful warfare. When defending cyber infrastructure, a creative army is needed to keep the defense mechanisms up to date and to innovate novel resilient defenses to counter constantly developing threats. Passionate people are also needed to defend cyberspace. Max Weber's notion of the state claiming a monopoly of use of force [33] is becoming obsolete, and one reason for this is that in cyberspace anyone can pick up weapons and become involved in warfare. It is also increasingly important for all sectors of society to be passionate about positive cyber security culture. In an interconnected cyberspace coupled with the physical world, it is essential for all stakeholders to cooperate in improving security.

Finally, there are a couple of limitations in the approach we have proposed in this paper. Clausewitz's work does not mark end of history and cannot explain all characteristics of modern cyber war in detail. Although Clausewitz does note that the nature of war is continuously changing, it is only one lens through which cyberwar can be observed. Moreover, On War contains many outdated sections that are not applicable to modern warfare. Still, at least for the technical aspects of cyberdefense we have focused on, the Clausewitzian principles of warfare provide a useful framework for further discussion between different fields of science.

5 Conclusion

This paper has argued that most of the fundamental tenets Carl von Clausewitz presented about warfare in his influential book *On War* can be applied to cyberwar to get a new multidisciplinary perspective on the topic. We have further shown how Clausewitz's theory on uncertainty

and friction in the war and his ideas of defense as a stronger form of warfare can be used to build a conceptual framework for proactive cyberdefense. In this approach, we combined Clausewitz's theoretical ideas with technical cyber defense solutions, which can help policy makers, political and military scientists as well as cyber security specialists to reach a common understanding of defensive cyber security.

References

1. Almäng, J.: War, vagueness and hybrid war. Defence Studies 19(2), 189–204 (2019)
2. Almeshekah, M., Spafford, E.: Planning and Integrating Deception into Computer Security Defenses. In: Proc. of the 2014 workshop on New Security Paradigms Workshop. pp. 127–138. ACM (2014)
3. AVTest: Malware statictics. https://www.av-test.org/en/statistics/malware/, accessed: 2019-08-20
4. Brantly, A.: The violence of hacking: State violence and cyberspace. The Cyber Defense Review 2(1), 73–92 (2017)
5. Bunker, R.: Five-dimensional (cyber) warfighting: Can the army after next be defeated through complex concepts and technologies? Report. Strategic Studies Institute, 1998.
6. Canabarro, D.R., Borne, T.: Reflections on the fog of (cyber) war (2013)
7. Clarke, R., Knake, R.: Cyber War: The Next Threat to National Security and What to Do About It. Ecco (2011)
8. Clausewitz, C.v.: On War. Princeton University Press (1989)
9. Cohen, F.: Operating system protection through program evolution. Computers & Security 12(6), 565 – 584 (1993)
10. Enterprise, H.P.: Internet of things research study (2015)
11. Falliere, N., Murchu, L., Chien, E.: W32. stuxnet dossier. White paper, Symantec Corp., Security Response 5(6), 29 (2011)
12. Farwell, J., Rohozinski, R.: Stuxnet and the future of cyber war. Survival 53(1), 23–40 (2011)
13. Garard, O.A., Friedman, B.: Clausewitzian alchemy and the modern character of war. Orbis (2019)
14. Gartzke, E.: The myth of cyberwar: Bringing war in cyberspace back down to earth. International Security 38(2), 41–73 (2013)
15. Heuser, B.: Reading Clausewitz. Bimlico (2002)
16. Huang, Y., Ghosh, A.: Introducing diversity and uncertainty to create moving attack surfaces for web services. In: Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats, pp. 131–151. Springer NY, NY (2011)
17. Imperva: Breaking Down Mirai: An IoT DDoS Botnet Analysis. https://www.imperva.com/blog/malware-analysis-mirai-ddos-botnet/, accessed: 2019-08-20
18. Jacobsen, J.: The cyberwar mirage and the utility of cyberattacks in war: How to make real use of Clausewitz in the age of cyberspace. Report. Danish Institute for International Studies, 2014.
19. Koselleck, R., Presner, T.: The practice of conceptual history: Timing history, spacing concepts. Stanford University Press (2002)

20. Larsen, P., Homescu, A., Brunthaler, S., Franz, M.: SoK: Automated software diversity. In: Security and Privacy (SP), IEEE Symposium on. pp. 276–291 (2014)
21. Lawson, S.: Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the united states. First Monday 17(7) (2012)
22. Lesk, M.: The new front line: Estonia under cyberassault. IEEE Security Privacy 5(4), 76–79 (2007)
23. Rauti, S., Leppänen, V.: A survey on fake entities as a method to detect and monitor malicious activity. In: 2017 25th Euromicro International Conference on Parallel, Distributed and Network-based Processing (PDP). pp. 386–390 (2017)
24. Rauti, S., Laurén, S., Hosseinzadeh, S., Mäkelä, J.M., Hyrynsalmi, S., Leppänen, V.: Diversification of system calls in linux binaries. In: International Conference on Trusted Systems. pp. 15–35. Springer (2014)
25. Rid, T., Buchanan, B.: Attributing cyber attacks. Journal of Strategic Studies 38(1-2), 4–37 (2015)
26. Robinson, M., Jones, K., Janicke, H.: Cyber warfare: Issues and challenges. Computers & security 49, 70–94 (2015)
27. Rõigas, H.: Cyber war in perspective: Lessons from the conflict in ukraine. In: A Civil-Military Response to Hybrid Threats, pp. 233–257. Springer (2018)
28. Satchidanandan, B., Kumar, P.R.: Dynamic watermarking: Active defense of networked cyber–physical systems. Proceedings of the IEEE 105(2), 219–240 (2016)
29. Spitzner, L.: Honeypots: Tracking Hackers. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA (2002)
30. Stone, J.: Cyber war will take place! Journal of Strategic Studies 36(1), 101–108 (2013)
31. Strand, J., Asadoorian, P., Robish, E., Donelly, B.: Offensive Countermeasures: The Art of Active Defense. CreateSpace Independent Publishing Platform (2013)
32. Thomas, R.: Cyber war will not take place. Journal of Strategic Studies 35(1), 5–32 (2012)
33. Weber, M.: Politics as a Vocation. Fortress Press (1965)
34. White House: International Strategy for Cyberspace. 2011.
35. Yuill, J., Zappe, M., Denning, D., Feer, F.: Honeyfiles: deceptive files for intrusion detection. In: Proceedings from the Fifth Annual IEEE SMC Information Assurance Workshop, 2004. pp. 116–122 (2004)
36. Zheng, Z., Reddy, A.: Towards improving data validity of cyber-physical systems through path redundancy. In: Proc. of the 3rd ACM Workshop on Cyber-Physical System Security. pp. 91–102. ACM (2017)