***CyberWarfare: The impact on military strategy***

***Jacob Cagle***

***POLS350T***

***Mr. Karp***

***4/29/24***

***Introduction***

Cyberwarfare is the use of strategic digital attacks against a nation state. The aim of cyberwarfare is to damage/disrupt computer systems. CyberWarfare refers to the effort taken by nations/organizations to compromise the computer networks. CyberWarfare aims to damage disrupt infrastructure using various methods of engagement.

CyberWarfare is a form of conflict that has recently emerged, where nations/organizations strategically/tactically deploy digital attacks to achieve specific objectives against foreign adversaries. This new form of warfare is primarily based on the infiltrating and manipulating of systems to gain access to information. The intention behind cyberwarfare attacks can vary from the disruption of adversarial infrastructure to the stealing of classified information. One of the most common ways cyberwarfare is carried out is through the use of Malware. Malware (malicious software) is a type of code or software that is created with the intent to cause harm to external systems. Malware is the most common way in which a cyberattack is carried out, mostly because the term malware is an umbrella term that includes ransomware and spyware. These types of attacks can spread across multiple computers after only compromising one. This explains why cyberwarfare is effective today, because information can be compromised and intel can be gathered in an instant.

The fundamental strategy of cyberwarfare is broken up into two main aspects of offensive cyber operations and defensive cyber operations. Offensive cyber operations focus on attacking the adversary to achieve a political goal or complete acts of cyber espionage like stealing information. An act of cyberwarfare in the scope of the United States has to be authorized similar to conventional attack. Offensive cyber operations can look like exploitation and disruption. Exploitation could look like identifying vulnerabilities within an adversary’s system and targeting that. Defensive cyber operations are measures that prevent/mitigate the use of offensive weapons on digital networks. Some examples of defensive operations have to do with cybersecurity and implementing procedures that would help minimize damage.

Cyberwarfare over the past couple of decades has emerged as one of the focus points for militaries across the globe. This focus point emerged from the importance of gaining control of cyberspace, and providing additional means tactically that militaries can use to make operations more effective. The increased use of cyberwarfare has had impacts that can be seen globally. Cyberwarfare has affected some aspects like security and international relations. With the cyber domain having this much of an impact, nations realized the importance of cyberwarfare and the potential implications that this way of warfare will have on the future of the world.

Throughout the completion of this paper I researched the topic of cyberwarfare through the use of books, articles, case studies, and editorial articles/papers. I also utilized previous knowledge gained from prior interest in the topic to aid my writing and structure of this paper. With the research that was done throughout the making of this paper, I have concluded that Cyberwarfare has grown in importance and relevance in the warfare domain. Militaries have begun to rely on cyberwarfare, and thus the cyber domain will become exponentially more important in the future than it is now as it relates to political and information warfare.

***Sloss - Arms Race***

Firstly, Sloss refers to arms race theory during the Cold War, in which two nations are competing to develop and rapidly deploy nuclear weapons. Sloss states that this old nuclear arms race is over, and a ‘new’ arms race has emerged. This new arms race involves what Sloss deems as the new security environment. This new security environment comes from a change in arms race when previously two countries would compete against each other with similar power. Now this ‘new’ arms race occurs between two or more countries and various weapons. Sloss brings up the point that countries like the United States have the advantage, but other countries like Russia and China, “are seeking ways to offset superiority”. (Sloss, p.1).

This ‘new’ arms race will require countries like the United States who have had sustained superiority and power over other countries to adapt their existing strategy with ideas like force planning and arms control. Thus, this will bring a new approach to arms control that revolves around transparency and mutual assurance. Mutual assurance between countries that would define where each country is at in terms of capabilities, and the giving each other the ability to question as well as state any reservations. Transparency is used to mitigate mistrust between countries and as a means to reduce tensions.

Furthermore, in this new arms race, the future of deterrence needs to be dominated by non nuclear forces. Countries like the United States need to develop a more in depth approach that looks at deterrence as more than just nuclear weapons. This new approach needs to include non nuclear deterrence and a wide range of defenses. This new idea of non nuclear deterrence can look like cyberwarfare.

Sloss continues with his point on tailoring deterrence strategies to each adversary that a country would run into. This would include adjusting non nuclear weapons that would effectively match up well against adversaries. This would be using various weapons that refers back to Sloss and his ideas on on a ‘new’ arms occuring. This new arms race occuring is going to include many countries and using various non-nuclear weapons.

Sloss and his ideas will predict a future where non-state and third party organizations will have more of an impact on the world and world powers. In the context of cyberwarfare, we see this occurring right now with third party organizations being hired by world powers to maintain non-attribution. Cyberwarfare is the future and is a non nuclear weapon that will challenge the existing world powers.

Sloss states the U.S. Security Policy will need to adjust their security policy and this will be important to mitigate the potential implications caused by the new arms race. The United States will need to have an adaptable security policy, so they adjust to the new environment that will see smaller countries play a bigger role in the future of wars. These smaller countries will play a bigger role in the future by using non nuclear weapons like cyberwarfare to offset the military capabilities that they don’t have in comparison to the large countries. The use of cyberwarfare in specifics will allow this to occur because this type of warfare is readily accessible to anyone as long as they have a computer. We can already see that this is already starting to happen with countries like Ukraine which I will talk about later in the paper.

If bigger countries do not adapt their security plan, smaller countries will use technology like cyberwarfare to lessen the gap.

***Posen - Doctrine***

Posen focuses on military doctrine which is responsible for creating critical components for a country like national security components. Posen highlights the term grand strategy and he defines this as likely threats that pose risk to a state’s security and how it can devise a plan to combat/mitigate this potential risk. This plan to mitigate this acting threat usually includes a politically and militarily way to combat this threat. This is mentioned by Posen because he uses this idea of grand strategy to explain “military doctrine”. General specifics on how a military should be employed and structured in response to this potential threat. This would usually include cooperation between different types of forces stated by Sloss. However, military doctrines sometimes will not incorporate political objectives or a grand strategy.

Countries stress one type of force instead of another, this could be for political or technological reasons for example. Within these forces certain weaponry is focused upon. For example, Posen stated that an Army might focus on short-range. While an Air Force might focus long-range attacks. These choices that those forces make are commonly known as *tactics.*

Furthermore, Posen breaks military operations into three categories. These three categories are offensive, defensive, and deterrence. He defines offensive doctrine as a means to disarm/destroy an adversary. While he defines defensive doctrines as a means to deny an adversary's goals and overall objective. Lastly, deterrence aims to raise the cost to an adversary while coming to a cost to its own military.

This idea of doctrine presented by Posen is important for reasons. Posen states that doctrine is important because the effectiveness of said doctrine will have an impact on the quality of “international political life”. The effectiveness of their offensive, defensive, and deterrence doctrines will increase/decrease the probability of a war. The effectiveness and adaptability of a country's doctrine will also impact the security of its own country. This effectiveness/ineffectiveness will impact assets like available technology. If this doctrine is not adaptive/innovative in the creation of the planning this can lead to defeat in worst cases.

Posen ideas on military doctrine states if a state holds offensive doctrine, this may cause an environment between a state and their adversary that is intense. If a state arrives at an offensive doctrine and concludes there. This may lead to an environment where they have an advantage in attacking their adversary. Especially if this state only holds an advantageous offensive doctrine. Thus, offensive doctrines tend to contribute to arms racing.

***Clausewitz***

Firstly, Clausewitz defines war as, “War is thus an act of force to compel our enemy to do our will” (Clausewitz, p.1). This act of war is to compel our enemy to do our will, but also war is also used to disarm the adversary. In an act to force an enemy to do our will, this has to be done through putting an adversary in a situation where their current situation is more unbearable than conforming. Also, war is complex and changes frequently.

Clausewitz presents his ideas on what he calls ‘friction’. War is easy to understand and plan for when you have seen it firsthand, and even if someone hasn't, things look simple. However it is extremely difficult to plan and predict the future of war when it can’t be seen. War that is unseen is nearly impossible to predict when minor things happen. This concept is why it’s hard to plan for wars because this concept of friction separates real war from war that is planned for one paper. Friction is the force that makes the seemingly easy on paper so much harder to predict when real war occurs. Thus, a military planner must know how to have an understanding of friction to be successful in planning and executing a plan while staying adaptable to individual situations in war. Chance is another idea that often coincides with friction. Chance involves a given circumstance in any situation that cannot be controlled. These two concepts from Clausewitz are inevitable and will occur in war.

Furthermore, another concept from Clausewitz is Clauwitzian dialect. This Clauwitzian dialect refers to the action that militaries take to counteract another military action.

Also Clausewitz talks about why we fight war. We mainly fight war with politics in mind to achieve a political goal. It is stated similarly here by Clausewitz when he said, “... the reason always lies in some political situation, and the occasion is always due to some political object.” (Clausewitz, p.86) In the same political vein, we don’t often fight for survival, we as a world often fight for ideas. This idea may be an existing technology that has gone obsolescent, and a nation will keep holding on to that technology to keep an idea instilled within its nation. However, we can solve the problem of holding onto obsolescent ideas by using Clauswitzian dialect as mentioned before. In using clausewitzian dialect we can break this pattern of holding onto near obsolescent ideas by looking at how to counteract and create an antithesis to combat how an adversary conducts war. If countries rely on what Clausewitz says in their dialect a country can effectively move away from the problem of holding onto obsolescent technology.

Clausewitz also highlights the center of gravity which is a critical point of an adversary, that if weakened or manipulated can be critical in defeating an enemy. As it relates to cyberwarfare and the new technologies, the internet can be used in a manipulated way to sway public opinion during wartime in a certain country's way. A country can use this as a way to gain an advantage in war, especially since a country's people could be a country's center of gravity. If a country doesn’t have its people on its side for a war, a war may not be in its favor.

***Ukraine-Russian War***

The Ukraine-Russian War tallies as the seventh time Russia has used cyber operations in a war. In this war there has been an increase in cyberattacks, although the severity of this type of warfare has become stagnant. Cyberwarfare has yet to make a considerable impact on the war on the battlefield. However, cyber operations have made a monumental difference when we consider the political advantage and information warfare that is being manipulated. The Russian cyber operations in Ukraine have succeeded in spreading disinformation to Ukraine which helps Russia politically in the war. This is how cyberwarfare will impact the future of warfare through political means. Through this idea presented by the Russia-Ukraine war, this tells us that cyberwarfare is going to play a more important role in shaping how the future of warfare is fought.

Russian Cyber Operations in 2022 according to the CSIS research team included 47 cyber incidents through november of 2021 through may of 2022. Through the use of non-attribution, this number of 47 is likely indicative of what actually occurred in terms of cyber operations during this period of time. Initially, Russian attempts at cyber warfare were proven to be ineffective for them, even after being used frequently. When looking at the type of Cyberattacks Russia has been using it is aligned with their past efforts relating back to more of a disruptive approach to cyberwarfare, rather than a degrading approach. This use of disruptive cyberwarfare has revolved around cyber espionage campaigns. According to CSIS reports, Russian cyberattacks upon Ukraine in 2022 attributed to 57.4 percent towards a disruptive approach while cyber espionage accounted for 21.3 percent of the total incidents. It is stated that Russia has failed once again to result in Ukrainian concessions. This use of cyberwarfare in the context of this war is relied upon to achieve efforts to gain intelligence information, rather than making a significant impact on combat operations.

This example of the ineffectiveness of what Russia is not doing in regards to cyber operation is not indicative to whether or not cyberwarfare is effective, but more so highlights the Russias failure to incorporate cyber operations effectively into their military operations/doctrine. The coordination with conventional forces as it relates to cyberwarfare is vastly important in making sure cyber operations are effective in a military plan. It is stated by CSIS that, “Russian military operations appear to struggle with integrating combined effects, especially across domains.” (CSIS, ) Like mentioned before, a military must coordinate between the planning and intel gathering stages to successfully integrate something like cyberwarfare into military operations on a large scale like Russia used in to combat Ukraine. These results found by CSIS, the Ukrainian government, and MIcrosoft can infer doubt that Russia didn’t effectively coordinate conventional and cyberwarfare, but cannot definitively back up this claim.

Conversely Ukraine is fighting a similar war versus Russia regarding cyberwarfare. As mentioned before, Ukraine was heavily attacked by a Russian onslaught of cyber attacks, but the Ukraine head of cyber operations at their security service stated that Ukraine held up against those attacks. Prior to the cyber attacks initiated by Russia, Ukraine got help from allies like the U.S. Cyber Command to help further their critical infrastructure to support the defense against Russia cyberattack. Some effort in attacking Ukraine is coming from Russian cybercriminals. This differing cyber offensive presented by Russia can help Russia reach places in Ukraine that Russia has been unable to reach prior to cyberwarfare. Russia for example has taken down television networks, in order to control the political views of people, but this has been thwarted by the Ukrainian government after quickly establishing the networks back online. Ukraine is fearing and preparing for Russia to start targeting the Ukrainian energy system and military communications. Like mentioned before, the ineffectiveness of the Russian cyberattacks can be attributed to their lack of coordination with conventional warfare. When Russia invaded Ukraine, Russia thought this war was going to be over within a few days/weeks, so the cyber operations were unsophisticated and easier to execute, thus Ukraine had an easier time mitigating these attacks.

As this war continues into the present day, Russia and Ukraine have the ability to adapt their doctrine to effectively incorporate offensive and defensive cyber operations. For example, in 2017 Russia launched the NotPetya attack that showed Russia that a cyberattack launched at one specific country can lead to it affecting other countries as well. The race is between Russia and Ukraine to see which country can take advantage of cyberwarfare to help aid them in cooperation with conventional warfare.

Arms Racing from Sloss pairs well with this cyberwar between Russia and Ukraine. The idea of a ‘new’ arms race pairs well because this new way of warfare in cyberwarfare predicted the idea that various actors will have an impact on war. Instead of this war being traditional in two nations competing in using one weapon, we see that in this war there are various non-nuclear weapons being used. In this certain instance cyberwarfare is being used by Russia offensively and by Ukraine defensively. In other cases where smaller countries are using offensive cyber operations, this is supporting the idea from Sloss that other countries are trying to offset their superiority. But as we are seeing in this war as we speak, Ukraine is mainly using defensive operations in an act to defend their networks and information.

This war supports Sloss in his ideas on using non nuclear weapons as deterrence. In this war, technology like cyberwarfare is becoming more of a deterrent and this is included in Sloss' ideas on a wide range of defenses to protect information.

However, this idea of a ‘new’ arms race and sloss’ ideas on tailoring strategies to a specific adversary is not shown in this war by Russia. As mentioned before, Russia used the same majorly the same type of cyberattack against Ukraine as they did against a country like Estonia. Russia was mainly using the same type of attacks like disruptive and cyber espionage attacks.

Inversely, Sloss' point on the use of third party or external organizations to aid a major nation in war was spot on in regard to cyberwarfare. In this war Russia used non-military cybercriminals to aid them in sending cyberattacks to Ukraine. Other examples have been seen around the world in non-wartime situations where countries will hire third party organizations to help them and attack and not get attributed back to them.

***OPM breach***

The OPM breach occurred in April of 2015 when the United States Office of Personnel Management (OPM) was compromised and millions of service members' information was lost to potentially malicious hackers. This initial action of the hack began back in November of 2013 when the group known at X1 first breached OPM networks. During this initial breach X1 was unable to get any personal information, but they were able to get the lay of the architecture of the OPM system. This opened the door for the X1 group, because the next month this group breach the systems of two government third party employers , Keypoint and USIS. These two third party government contractors conducted background checks on government employees and X1 gained access to the OPM servers through the USIS contractor. OPM didn’t even realize they were compromised until March of 2014. Instead of OPM publicizing the breach, they let the X1 hacker group stay in the servers to monitor what they were doing and gain counterintelligence on how they operated. However, this plan by OPM to wait and purge their networks failed because their system was infiltrated again when a group called the X2 used an access point from KeyPoint to establish a foothold on the OPM system. X2 did this by creating backdoor access into the system by installing malware into the network. Weeks later OPM did purge the system to remove X1, but did not detect the existence of X2 within their system. Later in July of 2014 the attacker extracted the information from inside the networks of the OPM systems. In October of the same year X2 breached an even more interior server that held the personnel information that was stolen. This attack included nearly 4.2 million people and data like SF-86 forms and fingerprints.

At the conclusion of this breach it is concluded that OPM’s leadership was too confident in themselves. After they initially purged their system and eliminated the X1 group, they thought that the infiltration was over. The OPM team failed to implement two-factor authentication which is important and was the recommended security standard at the time. This is just an example of how major world powers cna use cyberwarfare to infiltrate major classified systems to gather intel to aid them in wartime.

***Hive Ransomware***

The Hive Ransomware attack occurred in June of 2021 and is used by cybercriminals in target hospitals and energy grids for example. This hive ransomware is built to be distributed between cybercriminals and this hive ransomware could be utilized to support any political goal that someone would want to achieve. This ransomware attack occurs through the use of phishing emails that lures a victim into a link that infiltrates their system with this specific malware. Once infiltrated an actor will use multiple avenues to compromise their victims’ system. Cybercriminals would use a double-extortion tactic, which would look for ransom to get a decryption key, and a ransom to not spread the information across the internet.

It was crucial that countries/militaries infiltrated the Hive network to further secure the critical infrastructure of their nation and the world. The FBI did just that when in July of 2022 they infiltrated some of the Hive networks which helped ;ead to saving people who were being extorted over $130 million dollars.

In this case Cybercriminals use sophisticated technology to attack vulnerable people around the world. This Hive attack has compromised over 1,500 people and received over $100 million dollars from the victims. This Hive ransomware caused major disruptions within the critical infrastructure. For example, a hospital was infiltrated by Hive ransomware that caused people to be treated using old means and caused the delay of aid for people checking in with injuries. This could have been a by-product of death if someone was in critical condition. This has occurred before and should be looked at as a possibility when looking at the neglect of cyberwarfare.

Negatively affecting critical infrastructure in nation’s can lead to major financial losses which directly impact military function, as well as data integrity of a country. This Hive Ransomware is an example of how third party members that aren't affiliated with a specific country or a country that is small can have an impact on a future war.

This specific case looked at how cybercriminals got victims' information on a small scale. But if we look at this on a large scale and a military looks at this and uses this type of malware to gather intel on foreign countries. This could be done through the use of a government employee clicking on a phishing email, and then this spread into other important networks that could contain classified military information like the case above.

Posen pairs well with this case because of his ideas on doctrine. Posen states that military doctrine is responsible for creating security components. This includes security in the cyber domain, like mentioned in the above case. The United States played a big role in the previous and current counterdefense of this ransomware. For instance the United States worked with other countries like Australia to contain this ransomware to secure their critical infrastructure. An adaptable doctrine is crucial here to continuously assess and update procedures to actively defend against continuing cyberattacks. This is an example of what good can come from adaptable doctrine, and will be beneficial in future wars, when a country can learn from peacetime situations like third parties using Hive ransomware. For example, it is possible that the United States learned from the situation in the OPM breach to adapt their doctrine to fight against cybercriminals and nations in order to defend their critical infrastructure in this case.

Posen further states that doctrine will have an impact on “international political life”. This idea is presented well in this example because this Hive Ransomware affected over a thousand people and could have been much worse, and possibly led to critical informational components. However, the United States and other countries actively created planning and procedure to actively fight against this threat to critical infrastructure. In the future, the United States will need to maintain their security efforts against cyber threats like the Hive ransomware attack. Countries will also need to have an adaptable doctrine to combat future cyberattacks in peacetime/wartime.

***Course Theory that works the best***

Like stated above, I think the idea of an arms race works best with the cyber conflict between Russia and Ukraine. While this cyberwar between Russia and Ukraine doesn’t necessarily involve lethal means of using technology, nor doesn’t involve nuclear weapons. Arms racing still works well with the cyberwarfare between Russia and Ukraine are both trying to gain an advantage over the other. Both of these countries are trying to gain a continuous advantage over the other through the development of their cyber capabilities along with acquisition of new technologies that make new capabilities possible. Ukraine and Russia are in a competition to develop the most capable cyber technology that could push the advantage in gathering information. We can see in this war that once Ukraine thought Russia was increasing their cyber capabilities and was going to target their infrastructure prior to the Ukraine-Russian war, they went to increase their cyber defenses. This act to de-escalate the conflict and protect their information and fortify their vulnerabilities is resembling what would happen in a conventional act of arms race. This act for Ukraine to aid their cybersecurity can look like some type of deterrence to Russia and their offensive operations. Furthermore, countries like the United States went to aid Ukraine in cyber defenses before the cyber attacks started by Russia. While Russia used non-state actors during their cyber offensive operations to further increase their cyber offensive capabilities. The use of other alliances closely resembles what may happen in an arms race.

Specifically, Sloss states that in the ‘new’ arms race we will see the use of third party organizations to aid countries. This is happening currently in the Ukraine-Russian war, when Russia is using non-military forces in order to gain an advantage and bolster their cyber operations.

***Course Theory that works the least***

The ideas of doctrine by Posen/Hioback show that what the Russians did with their cyber operations against Ukraine was ineffective and worked the least. Like mentioned above, there is reason to believe that the ineffectiveness of the cyber operation on Ukraine can be attributed to their lack of adaptable doctrine. Their cyber operations and conventional warfare did not actively cooperate together to create a cohesive environment between the two. While Russia mainly used offensive cyber operations against Ukraine they failed at disarming/destroying adversarial capabilities. While some of the Russian plans involved political objectives like propaganda to spread disinformation, this was mitigated by Ukrainian cyber defensive operations. The Russian offensive cyber operations were not implemented into an adaptable doctrine, as Russia was using an existing plan from their cyber attack on Estonia. This approach consisted of mass amounts of attacks that they hoped would do damage, but only did minimal. If Russia would have had an adaptable doctrine in preparation of using offensive cyber operations against Ukraine they would have been more successful in their efforts. It looks as if Russia did not take the offensive cyber operations as seriously as other means of warfare in creating effective and adaptable doctrine. If they did do so, this war may have ended up in a different outcome at this point.

Since it’s untraditional in which the Russian’s are going about cyberwarfare, it has been difficult to implement effective doctrine by which their military forces could go about using it as a guiding action. This is possibly the case because this is intentional by the Russian military because they are using military and non-military operations to fight this cyber warfare. This can also explain why they didn’t use doctrine because it would be too costly or too time consuming for what they thought they should invest in a war against Ukraine. Some of these unconventional methods like mentioned above included disinformation waves by use of television networks.

As Hoiback states, adaptable doctrine can be an important step in making existing technology that was inoperable in military warfare, to something that is vastly effective. In the case of cyberwarfare, as this technology evolves and becomes more of a norm in military function, we will begin to see doctrine get established and see more of a support role from cyberwarfare in what this type of warfare will play in conjunction with conventional warfare. In this case, we saw what happened when Russia tried to use technology that is relatively new within the past few years without established doctrine. This attempt was mainly ineffective.The ideas of Hoiback on doctrine continue to not work so well. Hoiback states that for doctrine to be executed well, doctrine has to be the focus before the execution of a technology, and this was not focused on by the Russians beforehand.

***CyberWarfare/Course Theories***

As we can see through the use of theories like arms racing and doctrine, cyberwarfare will continue to play a supporting role in warfare. With doctrine we can see what can go wrong when doctrine in regard to cyberwarfare is not implemented properly with conventional warfare. Russia showed us how their cyber effects were ineffective if doctrine is not established. Inversely, we can see from the same example what can go right when Ukraine got some help from the United States. Ukraine got some basic doctrine that the United States had on defensive cyber operations that would be successful in defending against most of the Russian cyberattacks. In the future cyberattacks will become more effective if countries begin to align their cyberwarfare doctrine with conventional warfare and the already established objectives. As nations continue to use cyberwarfare, it will become easier to establish doctrine as we have more of an idea on what we can achieve with this technology. As this technology is relatively new, countries must be open to creating adaptable doctrine as it pertains to cyberwarfare because the more we explore the possibilities within this technology, the more change the more military doctrine will have to adapt to this.

When looking at cyberwarfare and how they go about conducting cyber operations, doctrine can tell us a lot about each country. The United States along with a country like Ukraine is more focused on information security and defensive strategy. These countries are more cybersecurity oriented, and look at offensive operations as a secondary priority. While countries like China and Russia are focused on defensive strategies,

While cyberwarfare is not the traditional arms racing technology because this type of warfare is not physical like nuclear weapons. Instead cyberwarfare is intangible and can sometimes be non-attributed back to the country of origin. Cyberwarfare can however be considered an arms racing technology because the competition is very real. The competition between countries to obtain the most capable technology is similar to a traditional arms race. However, like Sloss states in his ideas with a ‘new’ arms race there are multiple countries and groups that are using cyberwarfare. This increases the danger that can come out of cyberwarfare. While the impact of cyberwarfare is not kinetic, the impact on critical infrastructures can be monumental. Since the early 2000’s, the United States has been fighting against terrorism physically, but now groups like terrorist organizations can use this technology readably. Not only is it possible for terrorist organizations to use cyberwarfare, but individuals can use cyberwarfare at a high level as well. An organization down to an individual can exploit possible openings in a country's cybersecurity. This potential of impact, highlights the need to put assets towards cyberwarfare, and this has happened in the fast dew years. We have seen countries like the United States heavily invest in their future of cyberwarfare in order to protect their information against potential threats like countries and terrorist organizations.

Furthermore, the impact of cyberwarfare has increased year over year. So much so that cyberwarfare is beginning to negatively affect military operations more and more. For example, the Air Force confirmed that they have more than one million attacks in one day on their ground based systems. New innovations in cyberwarfare are growing and continuing to impact military operations. In the future, through the competition in arms race we might see the implementation of AI in cyberwarfare

Some of the ideas that Clausewitz brings up in ‘On War’ compare well and help us understand cyberwarfare. Firstly, clausewitz talks about the “fog of war’ which refers to ambiguity that may come with war. This relates well with cyberwarfare because the cyber domain is constantly changing and we lack some understanding of what can come out of using the cyber domain as an area of warfare. The offensive operations used by adversaries are hard to predict and in cyberwarfare an adversary only needs to find one way in to compromise a system. Furthermore, Clausewitz mentions friction which closely relates to cyberwarfare because there are many technical challenges that can come with this technology along with the newness of this way of warfare. Friction often occurs in cyberwarfare because of how complex the cyber domain is alongwith the rapid pace of which cyberwarfare is changing.

In addition to the above concepts mentioned by Clausewitz, he also talks about a center of gravity. Finding the center of gravity when in a war with an adversary could mean winning the war. In the context of cyberwarfare the center of gravity is likely going to be exploiting the enemy’s critical infrastructure. A center of gravity within a country may very well be its people. Being able to conduct information warfare by way of cyberwarfare, there is a possibility to spread disinformation throughout an adversary's country. This could help push a country's agenda and ultimately aid in winning a war. Another possible center of gravity for a country could be the information systems that holds all of the information on military operations/communication. If a country had the ability to compromise the operations/communication of another nation, this could provide a massive advantage that could aid conventional warfare.

***Future Trends/Conclusion***

In the future I think Artificial Intelligence will play a larger role in the cyber domain. This will ultimately affect cyberwarfare, and how we go about using cyberwarfare. I think smaller third-party organizations will be the first to experiment with this idea as they have more freedom as these independent entities aren't restricted. I think smaller entities who use offensive cyber operations like terrorist organizations will have a significant impact on the innovation of cyberwarfare. Continuing on future trends, I think quantum computing has the potential to revolutionize cyberwarfare. Through this quantum computing cyberwarfare has the possibility of being the future of warfare in general. If we as a world begin to understand the potential of quantum computing, this could change how we use the cyber domain.

Overall, my idea on cyberwarfare was that it was going to have a major impact on warfare in the coming years. However, after looking at cases like the Russia-Ukraine war, cyberwarfare is going to play a supporting role. Instead of cyberwarfare dictating a nation’s success in winning war, more importantly disregarding cyberwarfare will become a major reason for a country’s demise in war.

***Works Cited***

*Archuleta, Katherine. “Statement of the Honorable Katherine Archuleta, Director, U.S. Office of Personnel Management, Before the Committee on Homeland Security and Governmental Affairs, United States Senate on ‘Under Attack: Federal Cybersecurity and the OPM Data Breach.’” Committee on Homeland Security and Governmental Affairs, United States Senate, June 25, 2015.* [*https://www.opm.gov/news/testimony/114th-congress/under-attack-federal-cybersecurity-and-the-opm-data-breach.pdf*](https://www.opm.gov/news/testimony/114th-congress/under-attack-federal-cybersecurity-and-the-opm-data-breach.pdf)*.*

*Barry R. Posen, ‘The Importance of Military Doctrine’, in Posen,*

*The Sources of Military Doctrine (Cornell University Press, 1984), ch. 1.*

*Leon Sloss, ‘The new arms race’,The Washington Quarterly, Autumn 2001.*

*Carl von Clausewitz,On War, 1832, pp. 119-123.*

*Mueller, Grace B., Benjamin Jensen, Brandon Valeriano, Ryan C. Maness, and Jose M. Macias. “Cyber Operations During the Russo-Ukrainian War,” January 12, 2024.* [*https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war*](https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war)*.*

Harald Hoiback, ‘What is doctrine?’ in Dima Adamsky, ed.,

Contemporary Military Innovation (Routledge, 2012).

*“U.S. Department of Justice Disrupts Hive Ransomware Variant,” January 26, 2023.* [*https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant*](https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant)*.*

*Ovadia, Nadav. “Hive Ransomware Analysis.” Hire Ransomware Analysis (blog), February 15, 2023.* [*https://www.varonis.com/blog/hive-ransomware-analysis*](https://www.varonis.com/blog/hive-ransomware-analysis)*.*

Fruhlinger, Josh. “The OPM Hack Explained: Bad Security Practices Meet China’s Captain America.” CSO Online, February 12, 2020. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html.

Fortinet. “What Is Cyberwarfare? | Fortinet,” n.d. <https://www.fortinet.com/resources/cyberglossary/cyber-warfare>.

Digmelashvili, Temur (2023) The Impact of Cyberwarfare on the National Security. *Future Human Image*, Volume 19, 12-19. <https://doi.org/10.29202/fhi/19/2>

POLITICO. “Ukraine Gears up for New Phase of Cyber War With Russia,” February 25, 2023. https://www.politico.com/news/2023/02/25/ukraine-russian-cyberattacks-00084429.

———. “Cyber Operations During the Russo-Ukrainian War,” January 12, 2024. https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

I u

Brumfield, Cynthia. “U.S. Government Offensive Cybersecurity Actions Tied to Defensive Demands.” CSO Online, September 13, 2022. https://www.csoonline.com/article/573597/u-s-government-offensive-cybersecurity-actions-tied-to-defensive-demands.html.

McLaughlin, Jenna. “An Inside Look at Ukraine’s Cyber War With Russia.” *NPR*, September 4, 2023. https://www.npr.org/2023/09/04/1197548380/an-inside-look-at-ukraines-cyber-war-with-russia.

“U.S. Department of Justice Disrupts Hive Ransomware Variant,” January 26, 2023. https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.

Include Hoiback on what is doctrine.

Whiting, Nicola. “Cyberspace Triggers a New Kind of Arms Race.” *The Cyber Edge*, February 1, 2018. [https://www.afcea.org/signal-media/cyber-edge/cyberspace-triggers-new-kind-arms-race.](https://www.afcea.org/signal-media/cyber-edge/cyberspace-triggers-new-kind-arms-race.%5C)

“Defense Primer: Cyberspace Operations.” *Crs reports*, December 14, 2023. https://crsreports.congress.gov/product/pdf/IF/IF10537.

CrowdStrike. “10 Most Common Types of Cyber Attacks Today - CrowdStrike.” crowdstrike.com, April 3, 2024. <https://www.crowdstrike.com/cybersecurity-101/cyberattacks/most-common-types-of-cyberattacks/>.

Hughes, Neil C. “The Future of Quantum Computing: Predictions for 2024 and Beyond.” Techopedia, November 1, 2023. https://www.techopedia.com/future-of-quantum-computing#:~:text=%E2%80%9CWith%20the%20advancement%20of%20quantum%20computing%20and%20AI-driven,machine%20learning%20tactics%2C%20and%20AI-driven%20social%20engineering%20schemes.%E2%80%9D.