5-11-2016

Overlook of Sino-American Power Transition: With Special Considerations of Cyber Warfare

Dalton E. Runyon
Southern Illinois University Carbondale, drunyon20@siu.edu

Overlook of Sino-American Power Transition:

With Special Considerations of Cyber Warfare

Dalton Runyon

A thesis submitted to the University Honors Program in partial fulfillment of the requirements for the Honors Diploma

Southern Illinois University

13 May 2016

The international system has been under the influence of United States hegemony since the fall of the Soviet Union in the late twentieth century; however, in the past several years the strength of the hegemon has come into question. With the strength of the United States hegemony in question, the possibility of successors also comes into question. Although no current, clear-cut proof exists that China has the full potential to surpass the United States as the hegemon, China has shown the most potential of any single state. Most of this potential is due to China's large and ever-growing economy. With the possibility of American decline and Sino power rising, a fresh look needs to be taken at Power Transition Theory (PTT).

Regardless if China, or another state power, one day surpasses the United States as hegemon, transitioning away from a unipole has never occurred in the current international system. This requires special scrutiny when determining the possible outcomes of a transition. A new outlook on this theory is necessary because of the dawn of the Cyber Age. Cyber security and cyber warfare are going to play a major role in determining the results of the transition. The possibility of conflict revolves mostly around the how the challenger favors the current status quo, as dictated by the hegemon, or how willing the current hegemon is to concede its global status to the challenger. Previously, considering this possibility of conflict looked upon the status of each state's conventional military power: conventional weapons, man power, nuclear weapons. However, in the Cyber Age, conventional military power is not the only power that must be considered. China and the United States are two of the states that are most accused of international cyber attacks. Although never proven, the United States has been accused of helping to orchestrate the first-known intentional cyber attack, the Stuxnet virus, a topic that will be later discussed. However, both states are accused of daily cyber espionage against one another and others in the international system. This new and evolving power must be taken into

consideration when determining the outcome of an international power transition. This paper will argue that these cyber attacks will decrease the probability of an armed conflict and will be cause for a more peaceful transition. This paper will examine the effects of cyber warfare on PTT, as well as take into consideration possible other factors that could cause for a more peaceful transition. Along with the consideration of the effects of cyber warfare on PTT, a necessary look must be made at the effects of cyber warfare on Just War Theory (JWT). I will examine both of these effects as they concern the overall Sino-American relationship and the outcome of a possible power transition.

The current Sino-American relationship has most recently been defined by their economic trading partnership. According to federal census information, China is, and has been, the number one state that the United States has imported from, as well as the number one state that the United States has a trade deficit with.[1] This economic partnership mostly stems from the U.S.-China Relations Act of 2000 signed by then President Bill Clinton. The act allowed China to surpass Mexico as the United States' number two trading partner by 2006[2,] and by November 2015, China has surpassed Canada to become the United States' number one trading partner.[3] Similarly, the United States has moved into the position of number one trading partner for China.[4] If only viewed through an economic lens, the Sino-American relationship is very strong and would seem to deter any sort of conflict in a power transition. If a conflict were to occur, both states would take significant losses economically. The United States would lose nearly 28% of its imported goods,[5] and China would lose approximately $423 billion or approximately 19% of its overall revenue from exports. This also doesn't take into consideration possible embargoes from each state's military alliances, which would only further the economic losses for each state.

Although each state would take a significant hit economically during the conflict, special consideration needs to be taken of the large trade deficit that the United States has with China.

The possibility of conflict is highest during a power transition when the challenger reaches the condition of parity. The period of parity is defined as beginning when the challenger develops more than 80% of the resources of the dominant power and ends when the challenger exceeds the dominant power by 20%.[6] The growing trade imbalance of the United States is beginning to signify an increase in Chinese ability to produce its own many of its own resources. The United States at the end of 2015 had a trade imbalance of $365.7 billion with China. Although the United States does have a trade imbalance with its top eleven trade partners, the next highest imbalance is only 7$4.2 billion to Germany.[7] However, the trade imbalance with China has grown much more rapidly than any other state. If China continues to grow this trade imbalance, it may eventually enter the period of parity in which the United States would need to take a serious consideration of its trade imbalance if the state desired to maintain its position as hegemon.

However, there is other speculation that parity and overall economic prowess may not play as large a part in causing a power struggle. Preceding the First World War, the United States passed the United Kingdom in terms of the world's greatest economy.[8] Nonetheless, the United States did not become a great power in the international system until after the Second World War, a conflict that the United States and the United Kingdom were on the same side of. Part of this could be due to the United Kingdom's vast empire. But once the United Kingdom became the net borrower of the United States, the British Empire only lasted approximately another quarter of a century.[9] A similar effect could possibly occur if China surpasses the United States. United States has already become the net borrower of China; could the United States already be

in a position of decline without realizing it? The United Kingdom still continued through WWI, the interwar period, and most of WWII as the dominant power in the world, even though the system was more multipolar in nature than a hegemonic system. Other factors could have played a serious role in this as well, such as the United States' position of isolationism. The United States only entered WWI as a necessity to ensure the survival of Europe as a whole, and only entered WWII because of the preventive Japanese attack on Pearl Harbor. Although China was involved in an ideological proxy war with the United States during the Korean and Vietnamese Wars, since the end of the Cold War, China has mostly focused on economic relationships, not getting overly involved in conflicts in the Middle East or elsewhere. In fact most of the Chinese involvement, even during the Cold War, was based around the nation-building problems it faces today, not international conflicts. The current Sino-American situation shares these aspects with the previous British-American power transition; however, a major difference in the current situation is ideology.

The British-American transition occurred smoothly between the two countries. Although both countries were involved in a conflict during the time of transition, the two powers were clearly fighting on the same side of WWII. Many factors of WWII could have played into the transition. Britain came out of the war severely weakened and could not contest the United States even if it had wanted to maintain its position of power. Additionally, ideology played a major role in this transition. Although Britain likely did not want to give up its position of power, the United States had been a longtime ally of the British and shared the same core ideology of democracy. However in the possible Sino-American transition ideological similarities do not exist. The two states do share the strong economic ties, but China is still a communist country with a very opaque government and a highly-contested recent history of human rights violations;

all of which go against a core national interest of the United States. According the Robert Art, the United States has six core national interests: protect the homeland from attacks; keep the peace amongst Eurasian powers; preserve a stable supply and access to oil; preserve an open international economic order; spread democracy, the rule of law, and protect human rights; and avert climate change.[10] It is highly unlikely the United States would willingly allow for China to attempt to spread its ideology even if the United States was weakened by a conflict. Although there are now international organizations, such as the United Nations, that attempt to remedy these human rights violations, it is unlikely any of them could successfully deter against a unipole, as seen by the lack of effect of the United Nations' condemnation of the United States conflict in Iraq in 2003.

Although China and the United States have enjoyed a strong trading partnership, other aspects of international relations have not produced as strong of a relationship, which may cause China to attempt to change the status quo regardless of economic ties. One major area of dissidence is China's disagreement with the United States' policies in the Middle East. China has disagreed with the United States' involvement in the Middle East since the early 1990s. It is a general belief in China that the United States only got involved in the Middle East to extend its hegemony and secure a steady supply of oil. Most recently China accused the United States of this after the 2003 United States backing of regime change in Iraq.[11] China believes that the 2003 invasion of Iraq and subsequent ousting of Saddam Hussein were merely a ploy to create another democratic government in the Middle East, giving the United States more control and power over the region. The United States has vehemently denied these accusations and has some credibility to do so, as the number one state that the United States imports isn't a member of the Middle East or even of OPEC. The number one exporter of oil to the United States is its

neighbor to the North, Canada. China on the other hand relies heavily on the Middle East to obtain its oil. Saudi Arabia comes in at number one for China on the oil imports list. Although Saudi Arabia does come in as number two on the United States list of oil imports, it only makes up for 11% of total oil imports. Canada makes up 40% of total oil imports, and the top five is rounded out by Venezuela, Mexico, and Colombia making up 9%, 8%, and 4% respectively.[12] China does import a similar amount of oil from Saudi Arabia, approximately 16%, but relies on the Middle East as a region much more heavily. The countries of Saudi Arabia, Oman, Iraq, Iran, UAE, and Kuwait make up a combined 51% of China's oil imports. China's other major sources of oil come from Angola, 13%, Russia, 11%, and Venezuela, 4%.[13] With such a heavy reliance on Middle East oil, China needs to have a serious stake in the Middle East, more so than the United States.

If China is to enter the period of parity, it needs to ensure that it has control over the resources that it desires. If the United States continues to obtain this foothold in the Middle East, China may run itself dry of oil. As of 2015, China was producing approximately 4.25 million barrels per day with a consumption of almost 11million barrels per day.[14] Simple math shows that China is importing to make up approximately 6.75 million barrels of oil per day. If China were to lose its source of Middle East oil because of a conflict with the United States, it would lose the aforementioned 51% of imported oil and would fall approximately 3.37 million barrels of oil short per day. Although the United States has been involved in the Middle East for the past couple decades, it does not mean that the Middle East welcomes the United States. As a region, they have a mere 30% favorability view.[15] However, because the two states have invested themselves so heavily in the region, whether politically or economically, the Middle East will

likely become a region of contention between China and the United States in coming years if China wants to become the hegemon.

According to Alterman and Garver, China has two goals in the Middle East, expand friendly cooperation with all countries and obtain resources (mainly oil) and export markets.[16] Both of these goals can likely be accomplished through economic relationships. China has taken similar steps on the continent of Africa. China recognized the growing financial crisis that was affecting the West and took this time to make massive deals and transactions with African countries. In 2008, Beijing provided a stimulus package of $570 billion to the continent.[17] Although this stimulus package only strengthened Africa's dependence on commodities, it provided the necessary money to industrialize and increase mining production of the minerals that China required. By 2009, China's largest portion of FDI in Africa was mining at 29.2% of total FDI.[18] This investment into the continent has provided resources and political power for China.

China could very easily duplicate this process in the Middle East. The financial crisis in the West has since become much less of a problem, but China could still easily capitalize in the Middle East. As mentioned before, the Middle East's approval rating of the United States sits at a measly 30%, and China has already begun taking advantage of this. Unlike the United States which has been taking action in the Middle East for the past several decades to attempt to spread democracy and end the reign of dictators in the region, China has simply just had to verbally condemn the United States' actions to gain influence. China has denounced these actions by saying that it opposes outside states having influence and interventions in the region.[19] If China is capable of duplicating the process from Africa, it will likely look to Iraq first. Iraq has the fourth largest proven petroleum deposits, but the oil fields are underutilized.[20] Iraq does not have the

technological capabilities or funds to drill at full potential. China could easily duplicate the African process to aide Iraq in drilling for the oil and obtaining a vital resource for itself. Although this would only make China more reliant on Middle East oil, it would most likely have a much higher approval rating than the United States in the country.

China, however, must be very careful if it attempts to assert itself into the Middle East. The Middle East could very easily become a flashpoint between the United States and China, which would hurt China in two different ways. First, the United States has proven since the end of the Second World War that it is willing to bog itself down in conflicts over ideology. The Chinese should be aware of this because of the ideological proxy war in Korea that had the United States and China on opposite sides. In recent years, the United States has proven its willingness to continue this trend after the ten-year stint in Iraq for the spread of an ideology and the removal of Saddam Hussein from power. Second, China has to realize that a majority of its influence in the region is because of the stance it took on the United States' interventions. If China goes back on its position of no outside intervention, the Middle East could very quickly view China in the same light that the region views the United States, which would set China back even further.

China has proven that the Middle East is not its main concern. When President Bush and the rest of Washington, D.C., called on Beijing to assist in the War on Terror in the early 2000s, China attempted to leverage the situation. China originally said it would support the coalition if the United States provided concessions for Taiwan.[21] One of China's main goals currently is its regional influence in the Southeast Pacific, but the main problem lies with the United States' Seventh Naval Fleet stationed mainly in Japan. The United States pushed its way across the Pacific during WWII to fight the Japanese and has not removed itself from the region since.

According to the official fact sheet of the Seventh Naval Fleet, its purpose is to "maintain a continuous forward presence in the Indo-Asia Pacific, providing security and stability in the region."[18] The Seventh Fleet is also the largest of the United States Navy's forward-deployed fleets, which allows it to quickly react to possible conflicts in the region. China has reacted to this in recent years by creating "anti-access/area-denial" strategy to limit the naval power of the United States.[22] The strategy is to prevent the United States from even being able to get its fleet close enough to China's mainland to use its aircraft, let alone any sort of troop or naval bombardments. China is also attempting to increase its maritime power in the area. Although the United States has official diplomatic relations with the People's Republic of China and not Taiwan, it is still a major issue of tension between the two powers and could be another possible flashpoint.

One such instance of this tension in the South China Seas was the incident involving the *USNS Impeccable*, a small ship that is used to detect and track submarines. In 2009 the *USNS Impeccable* was stationed approximately 75 miles off the coast of the Chinese island Yulin to monitor movements of a new class of Chinese nuclear submarines.[23] The *USNS Impeccable* began to be harassed by Chinese ships even as it began to leave the area. The Chinese attempted to capture the towed sonar array of the *USNS Impeccable* until the United States sent a destroyer to the scene to escort the *USNS Impeccable*. The United States claimed that the ship was operating outside Chinese territorial waters. China claimed that foreign military ships were only allowed in the economic boundaries (approximately 200 hundred miles from shore) if their business was innocent in nature, and China did not consider the *USNS Impeccable* to be conducting innocent procedures.[24] Although this event may not have escalated into a naval conflict, this incident could have escalated tensions that could have affected political and

economic relationships between the two states. The amount of surveillance the United States and China conduct on one another is reminiscent of the United States and the Soviet Union during the Cold War. Regardless, China risked a lot by being so aggressive towards a surveillance-only ship. Although intelligence is very important in the military world, how much would China risk if it had been a United States ship with stronger military capabilities in its waters? And how much would China risk when it comes to Taiwan?

Overall the United States has been very critical of Chinese nation building. China has multiple concerns when it comes to unifying as one. China's main concerns for unification include Taiwan, Tibet, and the Muslim Uighurs. The United States officially switched its recognition of the Chinese government from Taiwan to the People's Republic of China on January 1, 1979. On this date the United States officially terminated the Sino-American Mutual Defense Treaty as well, since the treaty was created with the government in Taipei not the government in Beijing. Ever since then, there has still been speculation on whether or not the United States would defend Taiwan if China attempted to invade the island. On April 10th, 1979, President Carter signed into law the Taiwan Relations Act that includes provisions for the United States to provide Taiwan with "arms of a defensive character […] to enable Taiwan to maintain a sufficient self-defense capacity."[25] This does not call for direct protection if there is an invasion of Taiwan, but it also does not specify that the United States will not provide defense against China. As the hegemon, the United States has interfered in similar capacities elsewhere and could very easily do so in a Chinese invasion of Taiwan.

Taiwan isn't the only area of nation building that has brought criticism to China. China also has a problem with Tibet and the Muslim Uighurs. China illegally invaded Tibet in 1950 and has held it under occupation ever since. The West has since recognized Chinese sovereignty

over Tibet, but many charges of human rights violations have been made including genocide, which the United States and the West have intervened to stop before in other conflicts. China also has a major ethnic problem in the province of Xinjiang. Culturally the Uighurs that make up a majority of this province relate more to Central Asian countries than to China. In recent years there has been a large spark in violence amongst the Uighurs and the Han Chinese who are moving into the region. Many of the Uighurs claim discrimination, and a separatist movement has begun. China's nation building problem is a major one, and if the human rights violations continue, the West may attempt to interfere diplomatically, which could spark a conflict and a possible power transition.

A major hurdle that China would need to cross on its path through power transition would be the technological gap with the United States. Although China is moving closer and closer to surpassing the United States economically, it is merely exporting these new technologies, not creating new ones. The economic prowess of China has not translated into military prowess and technological prowess as it once did. According to World Bank data from 2013, the United States turned in $128 billion worth of receipts for innovation technologies; whereas, China turned in less than $1 billion worth.[26] Another indicator of technological prowess is the number of triadic patents; these are patents that are registered in the United States, Europe, and Japan. In 2012, the United States registered nearly 14,000 patents; whereas, China registered fewer than 2,000 patents.[27] Other indicators include examining the number of articles in science and engineering that appear in the top one percent of citations and number of Nobel Prizes won in science categories. The United States accounts for almost half of the papers in the top one percent of citations, eight times more than China, and has 114 Nobel Prizes in science since 1990, while China has two.[28]

Stephen G. Brooks and William C. Wohlforth in their article "The Once and Future Superpower" use these facts to argue that China is not approaching the United States economically and will not surpass the United States as the hegemon. However, these facts do not necessarily correlate with degrees of technological prowess. The authors fail to consider the role of globalization and how it affects the spread of new technologies. Although globalization does not affect the spread of all technologies, due to the classified nature of many government technologies, it can account for the spread of many everyday technologies. Globalization and technology go hand-in-hand. Globalization leads to the spread to the spread of technology, and better technology leads to more globalization. Much of this occurs not through state governments but through transnational corporations that operate outside governments. Although these technologies may not originate inside China, this does not mean China will not eventually obtain these technologies.

A major edge the United States has over China is its military prowess. The United States has had the strongest military and largest military expenditure for the past several decades, due mostly to its arms race with the former Soviet Union. China is catching up in quality of military technologies due to globalization. As stated, globalization does not help the spread of classified technologies of other states, but it does help the spread of technology that can be used to obtain said classified technologies. Cyber espionage and cyber warfare have revolutionized the international sphere, and the effects of this have yet to be considered in many International Relations theories. Thus far this paper has examined the relationship between the United States and China and how it affects the current method of examination for PTT; however, PTT was written several decades ago before this technological revolution. Cyber espionage and cyber warfare have already had profound effects on the international sphere as a whole, but its full

power has yet to be seen. Similarly the effects have yet to be seen on PTT. The abilities of cyber warfare allow for the curtailing of many conventional military operations and could potentially lead to the mitigation of conflict in a power transition scenario. Many arguments have been made that new world economic ties and military capabilities, such as nuclear warheads and democracy, have led to sustained peace, which would also affect the possible conflict in PTT, but cyber warfare also needs to be considered.

The capabilities of cyber warfare are countless: "everything from online protests to the stealing of internet secrets to cyber sabotage of nuclear research to battlefield acts of war."[29] As the world becomes more dependent on new technologies, the capabilities of cyber warfare will become endless. Militaries, utility grids, classified documents, identities, and countless more areas of our lives are stored or controlled digitally. For example, the United States has been deemed very difficult to invade due to the two large oceans on either side of its borders. But this only takes into consideration ground troops. Another consideration is the ability for other states to prelude invasions through cyber warfare. The ability to wipe out power grids, missile defenses, and opposing military capabilities makes such a ground invasion possible. Although countries like the United States definitely have cybersecurity to counterattack such measures, the possibility of being attacked is much more real.

The capabilities of cyber warfare can be seen through the 2010 discovery of the Stuxnet virus. The virus is believed to have originated from a joint American-Israeli operation. The virus was the most advanced malware known. The virus was active for approximately two years as the code dictated its own deletion on June 24th, 2012. The virus was created to attack only specific computers and was only spread to a set amount of computers. The virus was more than likely transferred through USB flash drives. Once inserted into a computer, the virus would search for a

Windows operating system; if found the next step was to look for either Siemens PCS7, WINCC, or Step7, all different software applications with industrial applications. Once done checking these criteria, the virus would spread to up to three computers on the same server. The target of the virus is believed to have been the Bushehr or Natanz nuclear facilities in Iran. Although the true target has never been confirmed, it is believed the virus was successful in attacking the Natanz nuclear power plant causing centrifuges to vibrate rapidly, thus damaging them and requiring replacements. The virus was successful in that it reached and destroyed centrifuges; however, it did not actually stop any uranium enrichment in Iran. The true effects of the Stuxnet virus are in the proven capabilities of cyber warfare. No malware has ever been as effective or secretive as this virus. By limiting the computers affected, the malware was much harder to detect and allowed for the completion of its mission. Similarly the fact that the Stuxnet virus is only believed to be of American-Israeli origin and has not been proven, shows how difficult is to defend against these types of attacks. Cyber warfare is silent but can be just as effective as conventional warfare.

The Stuxnet virus is a specific example of a SCADA attack. SCADA stands for Supervisory Control and Data Acquisition, a fancy term that means it is a type of industrial control system, which in turn simply means it monitors and controls physical industrial processes. SCADA servers are much more customized and require more complex codes and viruses,[30] hence the advanced nature of the Stuxnet Virus. SCADA attacks could easily target electrical power grids, communications, and the flow of petroleum.[31] Although no known SCADA attack on a power grid has occurred, the effects of such an attack can be seen in the 2003 major blackout of a large portion of the eastern United States and part of Canada. The blackout was caused by a chain of events that started with a simple software failure at a local

power plant that led to a local outage. The outage led to a strain on other local power plants that caused lines to sag and come into contact with trees, which in turn caused these lines to fail as well. After this the entire state of Ohio began drawing power from Michigan. Michigan's power grid was unable to sustain the load and began to fail in turn which led to power being drawn from more stations along the east coast causing failure after failure. In the end, 256 power plants were offline, and 55 million customers were without power.[32] A simple software failure and human failure to communicate led to one of the largest blackouts in history. If an attack on this grid had been intentional, much more damage could have been accomplished and loss of life could have occurred, especially if other utilities had been targeted as well. Although SCADA systems are highly customized, it is not difficult to obtain information on these systems, and attacks on such systems could cripple a state without sending in one ground troop.

Cyber warfare also allows covert activities to be done in a brand new manner. Covert activities no longer completely rely on infiltrating foreign governments by use of humans or double agents. Stealing of classified documents, eavesdropping, and denial of service attacks are some examples of cyber espionage. Although China appears to have been very successful in recent years in stealing highly classified military secrets, cyber espionage can also target large corporations. China is known to have cloned products, especially military products; they have cloned "bleeding edge U.S. aircraft including the Lockheed Martin F-35 Joint Strike Fighter and Northrop Grumman X-47B unmanned combat air vehicle (UCAV),"[33] as well as several land vehicles and small arms. China also clones products on much smaller scales: sandals, smartphones, alcoholic beverage, even some stores and restaurants. Cyber espionage has allowed for all of this. Although globalization would likely have led to some of this duplication, cyber espionage has allowed for much quicker advancement and creation of these products. Militarily

cloning was very difficult before cyber espionage due to needing the actual product to duplicate rather than retrofitting older products.

Another category of cyber warfare is Computer Network Attacks (CNAs). CNAs are defined as "actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves."[34] CNAs are the attacks that everyday citizens often consider when thinking of a hacker. Although hackers can create CNAs on a very small scale, the real danger comes from the capabilities of the state or state-backed entities. Along with a larger scale of attacks, the attacking state would likely "go for the throat,"[35] similar to a conventional attack. When non-state backed hackers commit CNAs, they only compromise the target in order to own it but do not take the full steps that may be required in actual warfare. For example, a hacker may break into a missile tracking system to gain access, but the hacker would not destroy or render the tracking system useless, unless it was a true act of war.

Cyber warfare also has profound effects on conflicts of conventional warfare. Cyber warfare can affect conventional warfare through two different categories: physically and electronically. Physically, cyber warfare effects troops on the ground. Some examples include the reliance of troops on new-age electronic technologies, supplies, and communications. Cyber attacks could occur against any or all of these categories which would render the troops to be less effective. A cyber attack that takes out an enemy's targeting systems or weapons leaves them unable to fight; take out their supply lines and they are unable to survive; take out their communications and they are suddenly alone. All of these are extremely detrimental to troops on the ground. However, these troops on the ground can prevent cyber attacks as well. Physical attacks can be carried out on power grids, communication lines, and other required processes to

keep computers powered and running. Without these the enemy may not be able to successfully utilize their cyber warfare capabilities.

The category of electronic warfare, just like physical warfare, can be affected by cyber warfare and can affect cyber warfare. Electronic warfare can be considered a subset of conventional warfare but is separate from the physical attacks.[36] Electronic warfare consists of attacks that take place on the electromagnetic spectrum. Electronic warfare can render cyber capabilities useless through the use of an electromagnetic pulse (EMP). EMPs destroy electronics, which would also render much of an enemy's infrastructure useless without a single physical blow. However EMPs and other technologies are themselves electronic, meaning that these weapons are just as susceptible to cyber attack.

Although cyber warfare is relatively new, states have already created defenses against these types of weapons. Many of these defenses fall into the realm of cybersecurity. States have people actively working to defend against these attacks. Whether its preventively, such as building firewalls, or reactively, such as stopping an occurring attack or espionage, cybersecurity is an ongoing occurrence that does not contain a method of deterrence like conventional warfare. Unfortunately, cybersecurity does not defend against conventional attacks against cyber capabilities. States have mainly two option to defend their cyber capabilities from conventional attacks, redundant infrastructure and hardening of facilities and equipment.

Redundant infrastructure consists of three types of backup sites: cold, warm, and hot. Cold sites are nothing more than a facility in which to renew operations. Utilities may need to be turned on, backup copies of data created and transported, building systems, etc.[37] Cold backup sites exist mainly in case of conditions that can be seen far into the future as it takes weeks or more to bring cold sites online. Warm backup sites are the next step up. Warm sites may have

some portion of the software and hardware as well as some systems and some connectivity, but backups would still need to be transported to the site and some configurations would need to take place.[38] It would only take a matter of days to bring a warm site online making these much more effective in case of a sudden attacks. Lastly, hot backup sites are completely redundant to an active site. This allows for almost zero data loss in case of an attack. Hot backup sites only require the personnel needed to run the site to begin operations, which can usually happen in a matter of hours.[39] All of these backup sites serve their own purposes, but overall each keeps the state's cyber capabilities protected and ready to resume operation in case of a conventional attack.

Facility and equipment hardening is similar to creating firewalls in cybersecurity. Hardening against conventional attacks is used to attempt to stop destruction of a state's cyber capabilities. In general hardening of structures and equipment refers to protection against EMPs. Although conventional attacks also include small arms and bombs, the structures that store cyber capabilities are generally already prepared for these types of attacks due to normal military codes and planning. EMPs however can very easily pass through these layers of concrete. Other basic protection includes fences and gates to prevent unauthorized entry, locks, traps, laminated glass windows, and the aforementioned structural reinforcements.[40] However, to protect the equipment itself requires much more advanced techniques. These techniques normally consist of shielding, faraday cages, waveguides, and different filters, to shield the equipment.[41] Overall these techniques simply alter the electronic currents from EMPs saving the equipment.

Another major question in cybersecurity and defense of cyber capabilities is whether to act reactively or proactively. The cybersecurity and protection methods against conventional attacks just mentioned fall into the category of acting reactively. These techniques fall under the

category of traditional warfare. Acting proactively may not fall into the paradigm of traditional warfare, but yet again brings up the debate of preventive versus preemptive warfare. As mentioned cyber warfare has yet to be considered as factors in many theories of International Relations and JWT is one of them. Much research can be done on the effects of cyber warfare on JWT, but this paper will only examine what is necessary to be considered in a power transition. Many proactive attacks can be made in advance, some even years in advance through both software and hardware. These attacks could easily be considered preventive and illegal, which is why JWT must be examined.

The Talinn Manual on the International Law Applicable to Cyber Warfare, published in 2013, created rules or guidelines for basics of how cyber warfare can and cannot be conducted. The main conclusions from this manual are:

- States may not knowingly allow cyber infrastructure located in their territory to be used for acts that adversely affect other States.
- States may be responsible for cyber operations directed against other States, even though those operations were not conducted by the security agencies. In particular, the State itself will be responsible under international law for any actions of individuals or groups who act under its direction. For instance, a State that calls on hacktivists to conduct cyber operations against other States will be responsible for those actions as if it had conducted them itself.
- The prohibition on the use of force in international law applies fully to cyber operations. Though international law has no well-defined threshold for determining when a cyber operation is a use of force, the International Group of Experts agreed that, at a minimum, any cyber operation that caused harm to individuals or damage to objects qualified as a use of force.
- The International Group of Experts agreed that cyber operations that merely cause inconvenience or irritation do not qualify as uses of force.
- States may respond to unlawful cyber operations that do not rise to the level of a use of force with countermeasures. Countermeasures are actions that would otherwise be unlawful were they not in response to the unlawful actions of another State. As an example, if one State disrupts communications in another, it would be lawful for the target State to respond by conducting disruptive cyber operations of its own.
- A State that is the victim of a cyber "armed attack" may respond by using force. The force may be either cyber or kinetic. In international law, an "armed attack" is a "grave" use of force. Any cyber operation that results in death or significant damage to property qualifies as an armed attack.

- The majority of the International Group of Experts agreed that non-State actors, such as cyber terrorists, are capable of conducting armed attacks, to which the victim State could respond in self-defense. In other words, the matter is not solely one of law enforcement. In certain circumstances, it would be permissible to use force against those cyber terrorists when they are located in other States.
- Under international law, it is possible that a conflict consisting entirely of cyber operations would qualify as an "armed conflict" to which international humanitarian law would apply. This is important because not only does international humanitarian law contain certain protections for individuals and objects during an armed conflict, but it also gives immunity to combatants for certain actions, such as intentionally killing the enemy, which would otherwise be unlawful.
- During an armed conflict, commanders and other superiors may be criminally responsible for ordering cyber operations that constitute war crimes or for failing to stop such operations when committed by their subordinates.
- Although there is no prohibition in international humanitarian law on civilians—such as hacktivists—conducting cyber operations during an armed conflict, if they do so, they sometimes become legitimate targets.
- Not all cyber operations directed against civilians and civilian objects are prohibited during an armed conflict. Instead, international humanitarian law primarily addresses operations that qualify as an "attack."
- The majority agreed that an attack is a cyber operation that causes injury or death to individuals or damage or destruction to objects or which interferes with the functionality of cyber infrastructure in a manner that requires repair. Therefore, these experts would conclude that cyber operations directed against the civilian population or civilian objects are not prohibited by international humanitarian law when they merely cause disruption, irritation, and inconvenience.
- Directing a cyber operation against a civilian is a war crime if it injures the civilian or was likely to do so.
- It is unlawful to use cyber attacks to spread terror among the civilian population.
- Cyber weapons must be the subject of a legal review before they can be fielded on the battlefield.
- It is unlawful to launch a cyber attack that is not directed at a lawful target and which therefore would indiscriminately cause damage to civilians and civilian objects.
- During armed conflict, cyber operations must be employed against a target if they are militarily feasible in the circumstances and would result in less harm to civilians and civilian objects than the use of conventional weaponry.
- The special protections that medical and religious personnel, medical units, and medical transports have under international humanitarian law apply fully with respect to cyber operations directed against them. The same is true with regard to "objects indispensable to the survival of the civilian population" like medical supplies, food stores, and water treatment facilities.[42]

Overall these key points show that cyber operations can be considered a use of force and the similar rules can be applied as they are applied to conventional attacks. Specific sections of JWT can also be examined for amore in depth examination as well.

The categories of Jus ad Bellum, which is the section of JWT that discusses if a conflict is justly initiated, can be used to show how cyber warfare will affect the possibility of a conflict in a power transition. Jus ad Bellum can be broken down into five categories: Right Authority, Right Intention, Probability of Success, Last Resort, and Proportionality. Cyber warfare could have a major effect on PTT, and it will most likely lead to either a mitigation or prevention of a conventional conflict between states.

Right authority of cyber attacks is difficult because according to right authority only states have the legal authority to wage war. Many nonstate actors have committed acts of war, i.e. ISIS, but cyber warfare allows even more people the capability to commit acts of war. By simply having a computer and some coding, independent actors could easily commit similar acts as a state would. Right authority, however, comes from national and international laws, treaties, and institutions. A major problem with this is that many states are not members of the same international institutions and many have very different national laws when it comes to the case of cyber warfare.[43] In a possible power transition conflict, one state could consider themselves to comply with right authority for cyber warfare attacks; whereas, another state's laws do not agree.

Right intention in JWT states that one can only use or threaten force for a just cause. The question is: how just is cyber warfare? The Stuxnet virus, if used correctly, simply attempted to stop uranium production in Iran, but does this justify a cyber attack in response? A large scale SCADA attack, for example, on a power grid could probably illicit a cyber attack in response, but does simple espionage illicit the same response? Or does it simply require diplomatic consequences? In a power transition this question will be the most difficult to answer. Right intention will be extremely hard to answer, possibly deterring a state from initiating cyber

attacks. Without proper knowledge of how to answer this question, it will likely be difficult to understand how the victimized state will respond.

Probability of success discusses that force must not be used in a futile war. Many of these again scenarios will not be simple to answer. The major question occurs what is considered a use of force when it comes to cyber warfare? For example again, the Stuxnet Virus did not harm any human life; it only attempted to stop the production of uranium in Iran, which produces the question: is this a use of force and does this even need to be applied to JWT?[44] In a power transition, probability of success is a major factor. If a challenger enters a conflict with the current superpower, it has to make sure it is able to win the conflict. Due to the former superiority of the hegemon, this will likely be very difficult to determine. Similarly if a former superpower attempts to start a conflict with the new hegemon, is it actually capable of winning the conflict? Due to the difficult nature of determining probability of success, it is likely that states will use cyber attacks against one another. Since the use of force is difficult to apply to cyber attacks, this could very easily replace conventional conflict.

Last resort is also very difficult due to the current definition of use of force. In power transition, last resort is very important. According to PTT, a conflict normally occurs because a challenger is unhappy with the status quo, or a former superpower is attempting to regain its spot as the hegemon. Neither of these are fit the right intention category and would likely need extensive diplomatic negotiations before a just conflict could even be remotely considered. Again cyber attacks will likely mitigate an actual conflict. Both the challenger and the hegemon likely will have the cyber capabilities to cripple the other's basic needs through SCADA attacks, which could easily replace a conventional attack and either secure or prevent a power transition.

Proportionality states that the benefits of warfare must outweigh the harms that are caused by it. Due to the unpredictable nature of cyber attacks, it will be difficult to determine proportionality. However, a large scale SCADA attack could be considered proportional if there is limited long-term damage and if it successfully deters further conflict between states.

Overall cyber warfare will have a mitigating effect on a conventional conflict, and this PTT must be reexamined and updated. Simple economic strength does not translate into military capabilities anymore, and military power does not directly translate into international prowess anymore. Another negative of PTT is that it merely assumes that a challenger wants to surpass the current hegemon. The world system recently left a bipolar world with the collapse of the Soviet Union leading us into the current unipolar world. Although PTT was written towards the beginning of the Cold War, long before the fall of the Soviet Union, it does not consider a continuation of a bipolar or multipolar world. Although it was very likely that only the United States or Soviet Union would come out of the Cold War as a sole hegemon, it does not mean the world system is destined to be a unipolar world, especially with the current state of globalization. Currently the world system is unipolar, but many of the major world powers are entrenched in massive military alliances and trade deals as well. These military and economic ties cause stronger bonds between states making conflicts much less likely. The question is: would NATO back the United States if it entered a conflict with China? Would it risk angering the possible new hegemon, or risk causing an all-out conflict between the United States backed alliances versus the China back alliances? These questions fail to be answered by the antiquated PTT. Although rivalries still occur in the world, such as the current Russian and United States rivalry that can be seen in the proxy war in Syria, it does not mean these states cannot work together for common goals. For example, global warming and terrorism are issues that cannot be solved by a

single unipole; it is going to take a worldwide effort to fix both of these issues. Is it not more beneficial for a multipolar world to rule? Another possibility is the creation of regional organizations. Already the European Union has shown it can be a force economically. Although it has had recent struggles with the strength of the Euro and the situation in Greece, it has accomplished the most important goal: peace. PTT must be updated in recent years to consider these possibilities. As stated International Relations theories need to begin to consider cyber capabilities and until then, the system of international laws will not be sufficient to truly determine just acts and the true nature of a possible power transition.

Endnotes

1. "Foreign Trade." *U.S. Top Trading Partners*. N.p., n.d. Web. Apr. 2016. <https://www.census.gov/foreign-trade/statistics/highlights/toppartners.html>.
2. "U.S. Relations With China (1949 - Present)." *Council on Foreign Relations*. Council on Foreign Relations, n.d. Web. Apr. 2016. <http://www.cfr.org/china/us-relations-china-1949---present/p17698>.
3. Stilwell, Victoria. "Cheap Oil Helps China Unseat Canada as Top U.S. Trade Partner." *Bloomberg.com*. Bloomberg, 04 Nov. 2015. Web. Apr. 2016. <http://www.bloomberg.com/news/articles/2015-11-04/cheap-oil-helps-china-unseat-canada-as-top-u-s-trade-partner>.
4. "China." Observatory of Economic Complexity, n.d. Web. Apr. 2016. <http://atlas.media.mit.edu/en/profile/country/chn/>.
5. "Foreign Trade." *U.S. Top Trading Partners*. United States Census Bureau, n.d. Web. Apr. 2016. <https://www.census.gov/foreign-trade/statistics/highlights/top/top1512yr.html>.
6. Zhu, Zhiqun. *US-China Relations in the 21st Century: Power Transition and Peace*. London: Routledge, 2006. p. 13. Print.
7. "U.S. Relations With China (1949 - Present)." Council on Foreign Relations. Council on Foreign Relations, n.d. Web. Apr. 2016. <http://www.cfr.org/china/us-relations-china-1949---present/p17698>.
8. Chan, Steve. *China, the US and Power-transition Theory: A Critique*. London: Routledge, 2008. p. 3. Print.
9. Sieff, Martin. *Shifting Superpowers: The New and Emerging Relationship between the United States, China, and India*. Washington, D.C.: Cato Institute, 2009. p. 68. Print.
10. Art, Robert J. "The United States and the Future of the Global Order." *US-China-EU Relations: Managing the New World Order*. Ed. Robert S. Ross, Øystein Tunsjø, and Tuosheng Zhang. Abingdon, Oxon, England: Routledge, 2010. p. 8. Print8
11. Alterman, Jon B., and John W. Garver. *The Vital Triangle: China, the United States, and the Middle East*. Washington, D.C.: CSIS, 2008. p. 12. Print.
12. "How Much Petroleum Does the United States Import and Export?" *Frequently Asked Questions*. U.S. Energy Information Agency, n.d. Web. Apr. 2016. <http://www.eia.gov/tools/faqs/faq.cfm?id=727&t=6>.
13. "China." U.S. Energy Information Agency, n.d. Web. Apr. 2016. <https://www.eia.gov/beta/international/analysis.cfm?iso>.
14. "China." U.S. Energy Information Agency, n.d. Web. Apr. 2016. <https://www.eia.gov/beta/international/analysis.cfm?iso>.
15. "Chapter 1: The American Brand." *Views of the United States and Foreign Policy*. Pew Research Centers Global Attitudes Project RSS, 14 July 2014. Web. April 2016. <http://www.pewglobal.org/2014/07/14/chapter-1-the-american-brand/>.
16. Alterman and Garver, *The Vital Triangle*, p. 19.
17. https://www.weforum.org/agenda/2015/03/what-the-shift-in-chinas-economy-means-for-africa/
18. "Chapter 1: The American Brand." *Views of the United States and Foreign Policy*. Pew Research Centers Global Attitudes Project RSS, 14 July 2014. Web. 08 May 2016. <http://www.pewglobal.org/2014/07/14/chapter-1-the-american-brand/>.

19. Alterman and Garver, *The Vital Triangle*, p. 112.
20. Alterman and Garver, *The Vital Triangle*, p. 47.
21. United States. Military. *The United States Seventh Fleet*. United States Navy, n.d. Web. Apr. 2016. <http://www.c7f.navy.mil/Portals/8/documents/7thFleetTwoPagerFactsheet.pdf?ver=2016-01-27-061248-087>.
22. Lai, David. *The United States and China in Power Transition*. CreateSpace Independent Platform, 2011. p. 118. Print.
23. Rapkin, David R., and William R. Thompson. *23. Transition Scenarios: China and the United States in the 21st Century*. Chicago: U Of Chicago, 2103. p. 1. Print.
24. Rapkin and Thompson, *Transition Scenarios: China and the United States in the 21st Century*, p. 2.
25. United States. Congress. *H.R.2479 Taiwan Relations Act*. Rep. Zablocki, Clement J., n.d. Web. Apr. 2016. <https://www.congress.gov/bill/96th-congress/house-bill/2479>.
26. Brooks, Stephen G., and William C. Wohlworth. "The Once and Future Superpower." *Why China Won't Overtake the United States*. Foreign Affairs, 27 Apr. 2016. Web. Apr. 2016. <https://www.foreignaffairs.com/articles/united-states/2016-04-13/once-and-future-superpower>.
27. Brooks, Stephen G., and William C. Wohlworth. "The Once and Future Superpower." *Why China Won't Overtake the United States*. Foreign Affairs, 27 Apr. 2016. Web. Apr. 2016. <https://www.foreignaffairs.com/articles/united-states/2016-04-13/once-and-future-superpower>.
28. Brooks, Stephen G., and William C. Wohlworth. "The Once and Future Superpower." *Why China Won't Overtake the United States*. Foreign Affairs, 27 Apr. 2016. Web. Apr. 2016. <https://www.foreignaffairs.com/articles/united-states/2016-04-13/once-and-future-superpower>.
29. Singer, P. W., and Allan Friedman. *Cybersecurity and Cyberwar: What Everyone Needs to Know*. New York: Oxford UP, 2014. p. 68. Print.
30. Andress, Jason, Steve Winterfeld, and Russ Rogers. *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*. Second ed. Amsterdam: Syngress/Elsevier, 2011. p. 141. Print.
31. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, p. 143.
32. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, p. 143.
33. "China's Military Built with Cloned Weapons." *USNI News*. US Naval Institute, 27 Oct. 2015. Web. Apr. 2016. <https://news.usni.org/2015/10/27/chinas-military-built-with-cloned-weapons>.
34. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, p. 181.
35. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, p. 181.
36. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, p. 182.
37. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners*, p. 148.

38. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* p. 148.
39. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* p. 148.
40. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* p. 149.
41. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* p. 149.
42. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* p. 222-223.
43. Andress, Winterfield, and Rodgers, *Cyber Warfare: Techniques, Tactics and Tools for Security Practitioners,* p. 250.