The Fifth Domain and its Effects on Target:

Cyberwarfare, Structural Realism, and the Democratic Peace Paradox

Sean M. Sarich
The Pennsylvania State University
Sjs6728@psu.edu
March 23, 2019

Author Note:

This paper has been prepared for PLSC 418W: International Relations Theory, Sect 001, Spring 2019, instructed by Professor Emma Leonard, Ph.D.

The Fifth Domain and its Effects on Target: Cyberwarfare, Structural Realism, and the Democratic Peace Paradox

ABSTRACT: Given the recent development of the digital conflict domain, aptly termed *cyberwarfare*, it is important for International Relations scholars to respond to this new conflict paradigm and appoint a narrative that both consolidates terminology and explores that validity of popular IR theories against the emergence of this new belligerence prototype. Given the common use of structural realism to rationally express meaning unto conflict among states, this paper contrasts the expression of cyberwarfare against the five straightforward assumptions that structural realism employs to explain the international system. The paper goes further by answering questions regarding the historical viability of using information technology to wage war and on to addressing structural realism's explanation of the immediate cyber-conflict mechanisms in the case studies of Russia, China, and Iran versus the United States under the umbrella of the democratic peace paradox. These case studies are then arranged using the *Stakeholder, Activity, Motive* (SAM) framework to clarify each actor, their assertive instances, and the purpose of these aggressions. What emerges from the case study analysis is support for the application of structural realism in identifying the security dilemma between democratic states and autocratic states as well as in accounting for the reactive progression of cyberwarfare doctrines between either regime type. Ultimately, these findings go on to confirm that structural realism provides a reasonable short-term explanation of the emergent "arms race" in cyber capabilities utilizing the pretense of the democratic peace paradox in the democracy v. autocracy dyad and the inclination of these regimes to reconcile the security dilemma by showing force, capability, and encouraging deterrence.

The Fifth Domain and its Effects on Target: Cyberwarfare, Structural Realism, and the Democratic Peace Paradox

Introduction

Ever since the first alleged state-sponsored cyberattacks took place on U.S. government agencies and contract assets at the hand of Chinese hackers in 2003, the very nature of interstate conflict has trended increasingly into a battle over 'ones and zeros' in lieu of the more analog tradition of guns and bombs (Bodmer et al, 2012). As of today, these emergent cyber threats have evolved in confluence with the ever-increasing reliance on and proliferation of information technology into just about every human domain. With such a wide technological adoption trend, the opportunity to exploit digital vulnerabilities has been noted by many state defense authorities that have previously relied on a 'boots on the ground' methods to either gain intelligence or subvert opposing threat actors. Among those authorities are those led by authoritarian regimes bent on supplanting the United States as the de facto hegemon driving the international system by employing the leverage and force multiplication offered by the global interconnection of information technology platforms. The obvious growth in media attention drawn by these actors and their cyber efforts has certainly been a product of an equal evolution of these nuisances into very real and damaging liabilities—something that has now made them and undeniable part of both domestic policy and the global conflict narrative.

In light of this fact, the U.S. and other democratic powers have termed a new conflict domain to address security concerns involving information systems dubbed *cyberwarfare*. Since the study of cyberwarfare is relatively new compared to more mature concerns within the international system, International Relations as a discipline must work quickly to codify the nature of cyberwarfare by vetting popular IR theoretical explanations against fast-evolving cyber conflict occurrences. In turn, it is posited that structural realism will offer the most pragmatic response to a state's adoption of a cyberwarfare doctrine, as the nature of cyberwarfare seems to

predicate itself upon the democratic peace paradox and the conflict-ridden relationship that tends to manifest itself between dyads involving both a democratic and an autocratic regime.

Literature Review and Hypothesis

To demonstrate the effect of structural realism via the democratic peace paradox on the cyberwarfare narrative, case studies examining cyber aggression between China, Russia, and Iran versus the United States have been utilized to fully understand the validity the aforementioned claims. These selections are not simply the product of arbitrary preference, but rather reflect the top 3 most aggressive cyber-threat actors according to a report released by the United States' Office of the Director of National Intelligence (via Strohm, 2018). Moreover, the fact that China, Russia, and Iran are non-democratic countries has lent interest towards the exploration of the democratic peace paradox and the prevailing shortfall of liberal theory in explaining the high likelihood of conflict that tends to occur between democracies and non-democracies. According to Thomas Risse-Kappen, "[w]hen liberal systems are faced with authoritarian adversaries, the complexity of democratic institutions appears to matter less" (1995, 499). This ultimately results in a security dilemma between both regimes whereby the nature of the regime matters little against anarchic survival tendency that structural realism cites as rational action on the part of either democratic or autocratic state leadership.

Since the de facto state of the democratic peace paradox results in the aforementioned security dilemma, the resulting prevail of structural realism likens itself well to what is currently known about the fledgling cyberwarfare paradigm. In a research paper produced by Valeriano and Craig, it has been codified that cyberspace is its own anarchic expanse with no sovereign to appropriate rules of conduct (2018). What results is an explanation of the veritable 'arms race' that seems to be occurring among state actors in increasing their offensive and defensive cyber

capabilities against the vacuous international system portended most prominently by structural realist theory. What remains is the hypothetical supposition that in the current infantile and anarchic state of cyberwarfare, structural realism will continue to account for the cyber 'arms race' observable between the democratic system of the U.S. and the non-democratic systems of China, Russia, and Iran.

Research and Methods

In order to compare the relationship between structural realism and cyberwarfare, one must understand the operative assumptions of the former's theoretical premise as well as the latter's qualitative aspects so that the two may be appropriately analyzed for commonality. In the case of structural realism, leading theorist John Mearsheimer has outlined five basic assumptions that substantiate the structural realist explanation. As for the qualitative aspects of cyberwarfare, the abstract nature of cyberspace itself requires a review of actions in order to give substance to the reason states would option for the use of cyber capabilities over more traditional implements of warfare. For this reason, the simple *stakeholder, activity, motive* (SAM) classification framework is employed and serves to organize the actions of states in juxtaposition to their overall motivations for acting in the first place.

In the interest in surveying the five assumptions of structural realism for their definitions, John Mearsheimer lists them in the following arrangement: 1) the international system is inherently anarchic, 2) all states have (some/minimal) offensive capability, 3) states are never certain of the actions of other states, 4) the main goal of any state is survival, and 5) all states are considered to be rational actors (Mearsheimer, 2013, 78-79). Stated plainly, the totality of these assumptions means that no one authority presides over the international system and thus states must constantly concern themselves with security against neighbors who may rationalize conflict in order to bolster

their own ability to survive. This security-based logic holds that any given state will opt for its own interest regardless of the luxuries afforded by alliance, identity, or morality as it views its own survival as prime and paramount over the welfare of others within the international system.

With regard to assembling the case study analysis of China, Russia, and Iran vs. the United States, the research material is intuitively arranged by using the SAM framework originally adopted by Kremer and Müller (2013, 41–58) to categorize the actions of the growing number of actors that affect the international system. Moreover, this same framework can be adapted to describe entities like terrorist factions and transnational corporations as wells as individual or groups of states. However, since the conflict paradigm being examined here is interstate, the default stakeholders become the states in question (i.e. China, Russia, Iran, and the United States). As such, the activities to be studied under this context will be the belligerent actions carried out by an offender in each dyad compared to the extent of their effect on the opposing state, others the international system, or both. This appraisal of actions then leads into perhaps the most important part of the SAM framework and its subsequent analysis by using the context of action or the outright statement of government officials to understand the motive of a particular actor.

By analyzing the assumptions of structural realism against the nonfigurative nature of cyberspace in the context afforded by the SAM case studies, both concepts can be held in juxtaposition and compared at a variety of levels. In the case of the assumptions of structural realism, the very arena of cyberspace may be examined for qualities that resemble the anarchic international system. This will help to elucidate the ‘wild west’ concept that is commonly associated with the recent nature of cyber conflict and why it might be coveted as a veritable mine of critical vulnerabilities by actors trying to reconcile a perceived security dilemma. Moreover, the establishment of realist dictates on behalf of the actors surveyed in the case studies will serve to

concatenate IR terminology in order to be applied to the analysis made substantive by the SAM framework. Inherently, if the supposition that structural realism is to be the dominant theory that describes the dyadic conflict method between U.S. democracy and the non-democracies of China, Russia, and Iran; then the structural realist principles should serve well to describe both the seemingly nebulous environment that exists within the abstract cyber ecosystem as well as help to define the warring paradigm that is characterized by the *cyberwarfare* appellation. Likewise, by using the sort of lane that is produced by the democratic peace paradox in instances of democratic-autocratic dyads, limitations of the research methods may be mitigated by focusing exclusively on testing the application of structural realist terminology in a relatively contained conceptual environment.

Structural Realism v. Cyberspace Analysis and SAM Case Studies

Beginning with very nature of the cyberwarfare, one must attempt to understand how the structural realist concept might be applied to an abstraction such as cyberspace if realist intellection is to be applied to higher concepts within the SAM framework. By comparing the innate aspects of cyberspace to the assumptions elucidated by Mearsheimer, the compatibility of cyberspace within structural realism's view of the international system may be vetted for analogy under the guise of the democratic peace paradox. In the following, this comparison is made between the current state of cyberspace and the five assumptions of structural realism trailed by an examination of the three case studies of China, Russia, and Iran vs. the United States.

Cyberwarfare v. Structural Realist Assumptions

The first realist assumption is that the international system exists in a state of anarchy. This means that there is no sovereign force overseeing state to state behavior or acting as an arbiter for global peace. This leaves states to vie for themselves in an international system made

up of other states that must be equally concerned with security in the absence of a peace-governing authority. Comparatively, in the abstract nature of cyberspace and the vast variety of devices connected to its ecosystem, there remains to be no conflict management body that oversees user behavior. Instead, there are only protocol authorities that govern compatibility and communication assurance across the infrastructural system that connects the many discrete networks of world (Craig and Valeriano, 2018). Plainly stated, cyberspace can be considered to be an anarchic landscape due to the absence of regulation provided by a higher authority. In many ways, this mimics the international system posited by structural realism in that both are at the whim of the action taken by actors or users in each respective system.

Regarding the second assumption of structural realism—that all states have at least some offensive capability—the application of the term *capability* becomes difficult to define in relation to cyberspace. While Isnarti (2016, 154) argues that '[a]nyone who can connect to computers and networks can conduct cyberwar' and that the comparison in sophistication to advanced weapons systems results in an extremely affordable and resource lean investment, there remains to be trouble in quantifying power in terms of cyber 'might.' The reason for this is because unlike bombs or physical munitions, it is difficult to understand the nature of cybersecurity investments as these faculties do not exist in a purely physical form. Craig and Valeriano (2018) use the example of increased offensive and defensive budgets allocated for U.S. Cyber Command to expound on this point. In this example, it is impossible to know if there is an actual investment being made into either offensive and defensive capability and to what lever of effect an investment would have in each. This differs from something like tracking nuclear weapons as there are various informative streams that lend indication to these types of programs, i.e. supply chain indicators, specialized personnel, remote radiation detection

capabilities, etc. In the cyber realm, technical prowess and the digital toolsets used for cyberoperations cause obscurity, though it can be postulated that any state with access to computers and networks can have at least some offensive capability under the extreme generalization afforded by Isnarti.

The aforementioned set of relative unknowns furnished by the difficulty in defining cyber capabilities directly supports the third assumption of structural realism: that states can never be certain about the intentions of others states. Alexander Lee (2018) asserts that the perceived cyber arms race is a direct result of the uncertainty model furnished by the obscurity of offensive and defensive cyber capabilities. This is reinforced by the seminal work of Robert Jarvis regarding the security dilemma in his argument that such a dilemma is heightened when offensive and defensive capabilities cannot be understood as two separate parts (1978, 199-206). The result of these unknowns is an increase in capabilities as a reaction without limitation, i.e. an arms race not unlike the stockpiling and strategic positioning of nuclear arms during the Cold War. The difference with cyberwarfare here is that once again its abstract quality allows for even more confusion over its capabilities, thus separating the degree of its severity from previous examples of arms races involving tangible weaponry.

Under the fourth assumption of structural realism, states operate with the main goal of ensuring their own survival. Whether the realist conventions of survival are based on stability in the international system (Waltz, 1964, 822, 907; Mearsheimer, 2013, 79-81) or in terms of power (Mearsheimer, 2001, 2; 2013, 79-81), both are hard factors to determine again because of abstract nature of cyberspace. While the veritable cyber arms race listed previously may indicate that states are clamoring for power within the cyber domain, the very few catastrophic cyber events available for reference tends to muddy the water with regard to what survival really

means in terms of an end state for cyber capabilities. In this particular assumption, however, there is indeed a direct overlap in the concept of state survival and the use of cyber offense and defense to ensure states survival from either the status quo or the power perspective. For this reason, this confluence of theory and conflict domain offers the strongest tether between each concept thus far even though the terms of survival may not be as clear as in historical examples of states invading other states or in the imagery of something as tangible as the threat of nuclear annihilation.

In its fifth and final assumption, structural realism supposes that all actors in the international system are rational and will maximize their chances of survival. In some ways, the merits of zero violence and the lack of a cyber "Pearl Harbor" indicate that major actors in cyberwarfare are behaving in rational ways. This is furthered by the emergence of rational choice and bargaining efforts within the international system that have ultimately indicated interstate deterrence and restraint (Valeriano and Maness, 2018, 264-265). It is of interest, then, that the neoliberal concept of bargaining asserts itself into the cyber self-help narrative that has to this point shown favor to structural realism. Neoliberal scholar Jennifer Sterling-Folker accounts for this in stating that neoliberalism theory mirrors the resource maximization principle of structural realism which would vouch for the cyber 'arms race' as well as cooperative measures between states to minimize acts of cyber aggression (2013, 115). John Mearsheimer (1994, 21), however, minimizes the appeals of liberalist theories in negotiation proceedings citing relative gains as the units of arbitration that do not hold weight in assuring overall survival. Sterling-Folker fires back at this criticism citing negotiation design as the shortfall and that large gains have manifested themselves in trade agreements after World War II and through the European Union (2013, 121). While the crude indication of rationality is implied in the lack of using cyber assets to attack

wantonly, the seemingly tangential reference to neoliberalism is important as its stands to indicate the possible intersection of competing theories into the cyberwarfare conflict narrative. In simpler terms, the cyberwarfare paradigm seems to be one of rationale in accordance with the assumptions of structural realism, however there may be more to the story than structural realism might offer. This emergence of conflicting theories shall be engaged in a later section, but it important to note that the literature often measures a history of negotiations as a means to determine rationality.

In analyzing the assumptions of structural realism against the nature of cyberspace, however, the first portion of the cyberwarfare narrative paints a picture of cyberspace as analogous to the anarchic landscape codified by structural realist theory. This precedent is important to the case study material as it identifies the underlying tethers that the real-world application of popular IR theories might have on emergent and/or abstract conflict domains. In this particular case, these assumptions may be weighed against the case studies of China, Russia, Iran, and the U.S. in order to ascertain the efficacy of structural realism in describing the deployment of cyberwarfare assets between the non-democratic v. democratic dyads featured in the democratic peace paradox.

Cyberwarfare Historical Premise and Case Study Analysis

As it pertains to the basic historical premise important for contextualizing the case study material, cyberwarfare as a concept has existed in movie references as early as *War Games* in 1983. In the movie, a young hacker finds a back door into a U.S. military computer network for which the hacker confuses nuclear fire control prompts with that of a yet to be released text adventure game. The unintended meddling results in the hacker inadvertently pushing the world to the brink of nuclear war before the hacker is recruited to undo the events that he set into

motion. It was not for another decade that the leaps in information technology and networking would lead to less dramatized ideas of what cyberwarfare could be and prompt the formative article *Cyberwar is Coming* by John Arquilla and David Ronfeldt. Noting the trends in interconnectivity and the automation of critical infrastructure via networking, Arquilla and Ronfeldt coined both the term *netwar* and *cyberwar* as a novel means to 'illuminate a useful distinction and identify the breadth of ways in which the information revolution may alter the nature of conflict short of war, as well as the context and the conduct of warfare' (1993, 24). The article went on to discuss the use of information technology as both an adjunct and a new vector for warfare with roots in the keen tradition of militaries to minimize uncertainty via intelligence and maximize command and control using innovative methods of communication. Yet, despite this intellectual entry, the first suspected state-sponsored cyberattack came another decade later when Chinese hackers would infiltrate unclassified networks at the U.S. Department of State, Department of Homeland Security, and Department of Energy in order to conduct a proof-of-concept through low-level espionage using basic network infiltration. This would set in motion events that would ultimately lead to the establishment and current state of the cyberwarfare domain and begin the cyber 'arms race' as it has been so noted previously ("Cyber Operations Tracker," n.d.).

As it pertains to the current inquiry, however, the SAM framework will be now utilized to analyze China, Russia, and Iran; noting their exchanges with the U.S. in terms of cyber-aggression and the motives that lead to the activity. This will culminate in a brief analysis against the assumptions of structural realism and what is known of each event's implication with cyberwarfare:

SAM Case Study #1: China v. the United States

Given the above-mentioned case of aggression dating back to 2003, China and the U.S. have been the longest standing case study in terms of cyberwarfare. Movement between these two countries in the cyberwarfare segment has been the impetus for distrust between both actors and has led both states to bolster their offensive and defensive cyber capabilities up to the present day. However, in order to understand China's role as a primary stakeholder in the cyber realm, one must understand the nature of China's cyber activity and the motives that seem to guide its actions.

To start, China's activities on the U.S. seem to hover predominantly around espionage in both state and corporate spaces. As of current, most of their attacks have been non-disruptive and involve stealing trade secrets and information of minor intelligence value. Many of the breaches have been against defense contractors and private industry within the U.S. with the intent to accumulate intellectual property and design insight on upcoming defense faculties. This is primarily for voluminous strategic intelligence gathering and to produce knock-off products that threaten the global market share of U.S. companies (Harold, Libicki and Cevallos, 2016, 6-8; Sherman, 2019). Of more imminent concern, however, are the growing number of breeches against companies tied to U.S. critical infrastructure—mostly in the gas transport sector. The intent of the Chinese here is largely unknown, yet the U.S. has heightened it concerns over these portions of critical infrastructure under the fear that China now has enough information on natural gas pipelines and perhaps other infrastructure to hold the U.S. gas and power supply under either full or partial hostage. (Harold, Libicki and Cevallos, 2016, 43; Clayton, 2013)

The motives of China in pursuing these digital campaigns against the U.S. are primarily rooted in political and power-seeking desires; classic of the assumptions held under structural realism. China has been noted to have a near obsessive aspiration to become a cyberspace

hegemon in response to the United States' de facto hegemony over cyberspace and even the international system. Moreover, the development and early adoption of the internet by the U.S. has led to global standards that are largely based on U.S. influence and commercial influence. As such, many internet governance groups and standardization authorities are rooted in the U.S. or in allied countries (ICAAN, ISO, IEEE, etc). China has come to view this alignment of standards as a threat to its own ability to control cyberspace as well as the broader narrative of global commerce and its online migratory pattern (Harold, Libicki and Cevallos, 2016, 28-30). Overall, cyberspace seems to be but one big part of China's larger plans to distribute more of the United States' power unto itself for no apparent reason other than to increase its stature in the international system.

Further supporting the structural realist explanations of China v. the United States in cyberspace is the cooption of nationalist hackers that has afforded China the ability to cloud attribution despite evidence of support by the Chinese government (Harold, Libicki and Cevallos, 2016, 30). The implications here is in the extension of China's state security concerns as something woven into the very fabric of its citizenry (Isnarti, 2015, 173-174). Mearsheimer elucidates on the importance of this, stating that '[t]he presence of nationalism, however, reinforces that balancing imperative, because then it is not simply the state's survival that is at risk, but the nation's survival as well' (2011, 35). The balancing that he is referring to is balance against a state's adversaries. In China's case, the weave of a corporate-like autocracy coupled with its ability to rear a deep nationalist sentiment only intensifies China's need to act in its own self-interests even if the reason for this action is not readily apparent to cultural outsiders.

SAM Case Study #2: Russia v. the United States

In the case study of Russia v. the United States, attacks against the U.S. have a fairly recent history and are known to be largely focused on espionage and social engineering for strategic and political purposes. Furthermore, attempts to gain access to sensitive data and leak it in opposition to political adversaries in the U.S. has been a looming concern since the mid-2010s. Perhaps the most obvious example of this is in the widely publicized controversy over the 2016 U.S. presidential election. During the election cycle, Russia is thought have sabotaged democratic front-runners at key points in their campaigns by leaking certain expository documents cultivated from a variety of hacks on the Democratic National Committee (CNN Library, 2019). Aside from targeting the U.S. political sector, recent cyberattacks have given cause for much higher concerns that once again center on the U.S. energy sector. A report furnished in 2018 revealed that Russian hackers were found to have infiltrated numerous gas and electric networks, to include that of an unnamed nuclear power plant. While the attacks seemed to focus on network reconnaissance, it was noted that the indicated primary goal was to gain access to the industrial control systems in each facility that would grant hackers (and Russian authorities) full control over either the production or destruction of any component attached to the network. This included the controls that keep nuclear reactors cool and from catastrophically failing such as in the infamous Chernobyl incident.

Given Russia's bent on controlling the U.S. political and energy sector, it would seem as though their strategy is not too dissimilar from that of China. Like China, Russia is using information technology as a lever to increase its stature on the world stage all while taking advantage of the swiftness, low resources, and obscurity it affords. This is outlined in its doctrine as part of *The Military Doctrine of the Russian Federation*, quoted as:

> [T]he prior implementation of measures of information warfare in order to achieve political objectives without the utilization of military force and, subsequently, in the interest of shaping a favourable response from the world community to the utilization of military force (via Connell and Vogler, 2017, 3).

Contrary to China's strategy, as evidenced by the above quote, Russia seems to be less concerned with the commerce side of the world and far more fixated on total power in its outright goal to achieve political and militaristic objectives. Moreover, Russia's cyber strategy as a means to defend against constant threats from both the international and domestic arena is further elucidated by Vladimir Putin himself. He uses the term *information warfare* to describe this new paradigm of espionage between states using new cyber toolsets and declares that "[p]rotecting Russia's information space against contemporary threats is a national security priority…" (Thomas, 2015, 262). By this measure, Russia's activity encompasses all non-destructive activity concepts as outlined in SAM as they attempt to steal trade secrets, influence public opinion, manipulate political structures, and seek to control critical infrastructure for strategic leverage. Their motivations thus become clear and are entirely power-related, political, ideologic, and economic (Kremer and Müller, 2013, 41–58). In the case of Russia v. the U.S., structural realism certainly lends context to the official doctrine furnished by Russian authorities, especially as outlined by their desire to use information technology to produce political outcomes such as in the 2016 presidential election and also in mobilizing U.S. government asset to react to threats on critical infrastructure. In total, the issue of balancing power is palpable in each move Russia has made in the cyber realm thus far.

SAM Case Study #3: Iran v. the United States

Iran presents a unique case study, as it showcases the first instance in the case study material where the U.S., along with Israel, were the initial aggressors. The U.S.-Israel coalition launched what came to be called the Stuxnet virus against the Iranian nuclear material refinement program in 2009. The attack was launched under the suspicion that Iran would use the refined nuclear material to build nuclear weapons instead of power plants like they had previously reported. Stuxnet went on to implement an undetectable bug in the SCADA system (industrial control system) that controlled refinement centrifuges. After causing small changes to the automated scheduled tasks within the industrial controls, Stuxnet would eventually produce an inexplicable excess movement in these spinning centrifuges, eventually causing them to go off balance and produce catastrophic failures and physical damage to the Iranian refinement facilities. Like the nuclear bomb before it, the use of malware to conduct a physical attack served as the second time the U.S. was involved in an attack that would come to legitimize an entire conflict paradigm. Today, Stuxnet is revered as the first state sanctioned cyberwarfare campaign that launched the first official cyber weapon to cause physical damage to a physical structure (Gross, 2013; Zetter 2015).

In response, Iran has since stood up the Iranian Cyber Army, a force that has now become the 4th largest cyber military unit behind those of the U.S., Russia, and China respectively. This is due in large part to the Stuxnet attack and has led Iran to launch attacks via state and proxy-run efforts on U.S. financial institutions (Kandell, 2018). Moreover, an interview with Behrouz Esbati, the top official in charge of Iran's cyber strategy, indicates that Iran is currently working to wholly define its cyber security strategy as well as its measures to retaliate against the west for the deployment of Stuxnet. In his closing remarks, Behrouz Esbati furnishes the following quote regarding the U.S.:

> "Nowadays, America is the symbol of the evil person and the Islamic Republic is the symbol of the divine person. There is no common ground for these two. One of these two must be victorious over the other." (Bucala and Pendleton, 2015).

The uniqueness of the Iran and U.S. dealing is that it is exemplary of the democratic peace paradox and affirms that the structural realist concept of the security dilemma is not above either the democratic or the non-democratic regime in a mismatched regime dyad. The U.S. and Israel have since been the only actors (as allies in Stuxnet) that have cause physical damage via offensive cyber capabilities. In the case of Iran, there efforts in the cyber domain have largely been retaliatory or at least are passable as such to the international community in light of Stuxnet.

Discussion

In review of the case study material, the structural realist explanation does act as a reasonable framework to describe the democratic vs. non-democratic dyad that fuels the democratic peace paradox. In each case study, the theme of balancing power or bolstering power in the name of self-service becomes obvious in the postural gains that motivated each state in their actions against the other. In the case of China, the pursuit of U.S. intellectual property, intelligence objectives, and control over the energy infrastructure in the United States is motivated by a deep nationalist ideology fixated influencing the international system the same way a top corporation in its category leverages market share against its competitors. In Russia, the goal is to social engineer the political outcomes in the United States in an effort to cause social instability while perhaps causing economic instability through compromising its energy sector. In either case, Russia would seek to implode American nationalism and perhaps the utilities that have become so relied upon as part of the U.S. consumer culture in order to increase

its own global power stature by decreasing the global power stature of its adversary. In case of Iran, the U.S. and Israel used social engineering and malware to curve the fate of Iran's nuclear program in spite of the fact that both the U.S. and Israel are themselves nuclear powers; powers that could be viewed as fearful of others having similar capabilities and thus preemptive in their tactics. As it can be seen, each action by each actor seeks an outcome that increases security through controlling aspects of other states through exploits in information technology.

However, while structural realism does offer a compelling explanation of the democratic peace paradox in these democratic-autocratic dyad cases studies, there are several week points that could benefit from further research. Principle among these avenues would be expanding this research to more dyads in order to challenge structural realism's use to demonstrate the repeatability of these outcomes. Additionally, and as alluded to in the research, there is room for overlap and explanation by other prominent IR theories. Liberalism in particular could do well to make sense of the tendency for states to negotiate outside of the vacuum of the particular issues of cyberwarfare in a world that is defined by more than one domain of militaristic conflict. Even so, the negotiations that have occurred between China and the U.S. specifically as they pertain China's willingness to come to the table over intellectual property concerns and cyberattacks is but one example that shows that negotiation within the domain is even possible (Mason, 2019). In another example, Power Transition Theory (PTT) can be used to understand the value in power imbalance while relating the probability of combat against the some of the tenets of realism. Yavuz Akdag (2018) makes a compelling case for this by describing realism in the static nature of cyberwar between China and the U.S. but then outlining how PTT might be used to predict actual war between China and the U.S. by understanding the distribution of economic, political, and military capabilities. Also, constructivism could weigh in on the highly abstract

nature of cyberspace to better understand the social valuation of an environment that is completely synthetic. In some ways, the tactics employed by the Russians seek to challenge long-standing institutions in the U.S. by leveraging social forces alone and would benefit from the constructivist take on the issue. In total, the young domain of cyberwarfare is in need of further research. In the immediacy, however, it seems that structural realist does an adequate job at explain the use of cyber capabilities among the democratic-autocratic dyads in the democratic peace paradox.

Conclusion

To conclude, structural realism has presented itself as a useful framework in codifying the cyber "arms race" narrative between dyads of democratic and non-democratic states. In the bigger picture, the structural realist arc shows value in describing young conflict domains as actors seek to understand the long-term implications of new capabilities and their effect on the international system. This addresses gaps in the research by demonstrating the value of popular IR theories in new conflict paradigms as well as the use of structural realism in explaining a domain that is still lacking in academic research compared to more mature issues in the international space. In this particular instance, the proliferation of information technology ensures that scholars need to continually test popular IR theories and perhaps even unify concepts in order to adequately address issues as complex and abstract as cyberwarfare.

References:

Akdag, Yavuz. 2018. "The Likelihood of Cyberwar between the United States and China: A Neorealism and Power Transition Theory Perspective." *Journal of Chinese Political Science*: 1–23.

Bodmer, Sean et al. 2012. *Reverse Deception: Organized Cyber Threat Counter-Exploitation*. McGraw-Hill.

Bucala, Paul, and Caitlin Shayda Pendleton. 2015. "Iranian Cyber Strategy: A View from the Iranian Military." *Critical Threats*. https://www.criticalthreats.org/analysis/iranian-cyber-strategy-a-view-from-the-iranian-military (March 4, 2019).

Clayton, Mark. 2013. "Exclusive: Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage." *The Christian Science Monitor*. https://www.csmonitor.com/Environment/2013/0227/Exclusive-Cyberattack-leaves-natural-gas-pipelines-vulnerable-to-sabotage (April 10, 2019).

CNN Library. 2019. "2016 Presidential Campaign Hacking Fast Facts." *CNN*. https://www.cnn.com/2016/12/26/us/2016-presidential-campaign-hacking-fast-facts/index.html (April 10, 2019).

Connell, Michael, and Sarah Vogler. 2017. "Russia's Approach to Cyber Warfare." *Center for Naval Analyses*. https://apps.dtic.mil/dtic/tr/fulltext/u2/1032208.pdf (February 25, 2019).

Craig, Anthony, and Brandon Valeriano. 2018. "Realism and Cyber Conflict: Security in the Digital Age." In *Realism in Practice: An Appraisal*, eds. Davide Orsi, J. R. Avgustin, and Max Nurnus. Bristol, U.K.: E-International Relations . essay, 85–102.

"Cyber Operations Tracker." *Council on Foreign Relations*. https://www.cfr.org/interactive/cyber-operations/titan-rain (March 24, 2019).

Gross, Michael Joseph. 2013. "Silent War." *Vanity Fair*. https://www.vanityfair.com/news/2013/07/new-cyberwar-victims-american-business (March 24, 2019).

Harold, Scott, Martin C. Libicki, and Astrid Stuth Cevallos. 2016. *Getting to Yes with China in Cyberspace*. Santa Monica, CA: RAND.

Isnarti, Rika. 2016. "A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War." *Andalas Journal of International Studies (AJIS)*5(2): 151.

Isnarti, Rika. 2015. "The Role of China's Patriotic Hackers and Their Relationship to the Government." *Andalas Journal of International Studies (AJIS)*4(2): 161–80.

Kandell, Shannon. 2018. "Iranian Cyber Warfare: State Repression and International Retaliation." *Compass*. https://wp.nyu.edu/compass/2018/11/13/iranian-cyber-warfare-state-repression-and-international-retaliation/ (March 4, 2019).

Kappen, Thomas Risse -. 1995. "Democratic Peace — Warlike Democracies?" *European Journal of International Relations*1(4): 491–517.

Kremer, Jan-Frederik, and Benedikt Müller. 2013. "SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World." *Cyberspace and International Relations*: 41–58.

Lee, Alexander. 2018. "Cyber Warfare and Theories of IR: Cyber Anarchy." *IPPR Blog: Cyber Warfare and Theories of IR Cyber Anarchy Comments*. https://blogs.ucl.ac.uk/ippr/cyber-warfare-and-theories-of-ir-cyber-anarchy/ (March 24, 2019).

Le Miere, Jason. 2018. "Russian Hackers Attacked U.S. Nuclear, Aviation and Power Grid Infrastructure, FBI and DHS Warn." *Newsweek*. https://www.newsweek.com/russian-hackers-us-nuclear-power-847267 (April 10, 2019).

Mason, Jeff. 2019. "Exclusive: US, China Sketch Outlines of Deal to End Trade War – Sources." *Reuters*. https://www.reuters.com/article/us-usa-trade-china-deal-exclusive/exclusive-u-s-china-sketch-outlines-of-deal-to-end-trade-war-sources-idUSKCN1QA07U (March 25, 2019).

Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. New York: W. W. Norton & Company.

Mearsheimer, John. 2011. "Kissing Cousins: Nationalism and Realism." https://mearsheimer.uchicago.edu/pdfs/kissingcousins.pdf (March 24, 2019).

Mearsheimer, John J. 2013. "Chapter 4: Structural Realism." In *International Relations Theories: Discipline and Diversity*, eds. Tim Dunne, Milja Kurki, and Steve Smith. Oxford University Press. essay, 77–93.

Sherman, Erik. 2019. "One in Five U.S. Companies Say China Has Stolen Their Intellectual Property." *Fortune*. http://fortune.com/2019/03/01/china-ip-theft/ (April 10, 2019).

Sterling-Folker, Jennifer. 2013. "Chapter 6: Neorealism." In *International Relations Theories: Discipline and Diversity*, eds. Tim Dunne, Milja Kurki, and Steve Smith. Oxford University Press. essay, 114-131.

Strohm, Chris. 2018. "China, Russia, Iran Top Cyber Threats, U.S. Intelligence Finds." *Bloomberg.com*. https://www.bloomberg.com/news/articles/2018-07-26/china-russia-iran-top-u-s-cyber-threats-u-s-intelligence (March 24, 2019).

Thomas, Timothy L. 2015. *Russia Military Strategy: Impacting 21st Century Reform and Geopolitics*. Fort Leavenworth, KS: Foreign Military Studies Office.

Valeriano, Brandon, and Ryan C. Maness. 2018. "International Relations Theory and Cyber Security." *Oxford Handbooks Online*: 259–72.

Waltz, Kenneth N. 1964. "The Stability of a Bipolar World." *Daedalus* 93, no. 3: 881-909. http://www.jstor.org.ezaccess.libraries.psu.edu/stable/20026863.

War Games. 1983. USA: MGM.

Zetter, Kim. 2015. *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York, NY: Crown Archetype.