What Do We Know About Cyber War?

Brandon Valeriano,
Bren Chair of Military Innovation
Marine Corps University
Senior Fellow, Cato Institute
drbvaler@gmail.com

Ryan C. Maness
Assistant Professor, Department of Defense Analysis
Director, DoD Information Operations Center for Research (IOCR)
Naval Postgraduate School
rmaness@nps.edu

Benjamin Jensen
Professor, School of Advanced Warfighting
Marine Corps University
and
Scholar in Residence
American University
benjamin.jensen@usmcu.edu

Introduction

Grasping what the international relations and security studies community knows about war also means grappling with how the conduct of wars will evolve in the future. Emergent technologies will play a role in reshaping the meaning of war as the character of conflict evolves over time. New tools and methods to wage battle and conduct statecraft below the level of armed conflict will inevitability alter what we know about the process of war, as well as the relations between adversaries in times of peace.

The current new technological advancement that has coercive potential is represented by the development of cyber operations. The challenge is that these new tools often come with vastly inflated potential, and generally fail to alter the course of warfare. As some propose, cyber tools offer a technology posed to reshape war and even the international system (Kello 2013, Clarke and Knake 2014, Kello 2017).[1] Cyber conflict is part of the present and will be a factor in the future of war, but this statement comes with many caveats.

Cyber conflict will not reshape war and will only move things at the edges, potentially increasing the ability of states to signal discontent. Cyber tools are unsure, limited in reach, mostly non-lethal, costly to develop, require a confluence of events to make them work, and generally are unable to shape the dynamics of battle (Valeriano and Maness 2014, Valeriano and Maness 2015, Kostyuk and Zhukov 2019). Cyber tools are poor means of compellence and deterrence (Valeriano et. al. 2018). They can offer an additive value in combat if offensive cyber operations can take out the command and control (C2) of the opposition or disable weapons platforms while in use, but the utility of the offense is dependent on the failure of the defense.

[1] A weapon is generally a poor term to describe digital packages with lines of code with unclear offensive and defensive abilities. Scholars are moving away from the term cyber weapons.

Although not as destructive in the physical realm, perhaps the relevance for cyber tools is found in operations in the information environment (OIE). If true, cyber-enabled information operations may be the force multiplier that states are seeking, where covert operations such as espionage and psychological warfare become critical wearing down the enemy's will to fight or reaching the domestic population. However, these are old tactics being utilized by a new technology, not a game changer for how states start or conduct war.

The shape of war remains resilient and new tools only reshape the contours of war, not the nature of the fight. Both offensive and defensive options based on emergent technologies offer great promise, but they often inevitability crumble when confronting the true brutality of war. The tank enables great maneuverability but is limited in production quantities, needs vast amounts of fuel, and remains a costly investment. Stealth bombers remain vulnerable to detection despite their name and are being utilized in sparing quantities in conflicts. Unmanned vehicles (UAVs) reduce the need for manned aircraft, but their main utility is loitering, reconnaissance, and not taxing the resources of the state deploying these forces.

The conjecture for some is how can be there be a decline in war when future technologies like cyber options -malicious digital weapons - will increase lethality and offer a means to continue the fight in new ways? This chapter will explore this question and review what we know about cyber conflict covering the nature of war, dynamics of coercion, escalation, and the possibility that these tools can limit the onset and exacerbation of conflict. Findings to this point suggest a limited potential of cyber technologies to transform what we know about war, but this does not mean that other technologies cannot reshape the future potential for warfare.

Cyber Operations and the Onset of War

For many, cyber security is a top national security threat and a challenge to the stability of society that requires a reorientation of national strategy. The mystery surrounding cyber operations shapes the perception that we are vulnerable to digital violence. The fear of the unknown animates many projections about the future of war. The potential for cyber operations to reshape war mystifies pundits and observers alike, but this threat is now over 35 years old. Cyber tools are not new weapons, the challenge is the ubiquity of the internet expands potential attack surfaces, giving the opposition more targets of interest. The other issue is that dependency on digital communication can now endanger command and control facilities making it impossible for leadership to communicate.

Luckily, the utility of cyber operations seems to be generally confined to fiction as presented in science fiction, such as Battlestar Galactica (Dykstra et. al. 2003), or popular fiction such as the novel Ghost Fleet (Singer 2015). Fiction has animated our beliefs about cyber operations, a key event being the release of the blockbuster film Wargames (1983), which prompted President Ronald Reagan to establish the first task force to examine our national cyber vulnerabilities (Kaplan 2016).

For this exercise, we define cyber conflict as "the use of computational technology for malevolent and destructive purposes in order to impact, change or modify diplomatic and military interactions between states." (Valeriano and Maness, 2015: 21). Many have suggested our future will be dictated by cyber conflict (Clarke and Knake 2014, Kello 2013) while others question the utility of cyber operations for war (Gartzke 2013, Rid 2013, Valeriano and Maness 2015). If we define war as an crises event between nation-states with 1,000 battle deaths (Small and Singer 1972), there is little probability of "cyber war" because cyber options have yet to be the direct cause of even one death.

It is possible that death and destruction can occur via cyber operations, but these sorts of dramatic attacks represent a massive escalation in intensity between states that would likely only happen if there is an ongoing major war. In fact, the only cyber operations that could provoke kinetic responses occur doing ongoing hostilities (Borghard and Lonergan 2019). What is more likely is that cyber operations will be utilized for sabotage (Rid 2013) or deception (Gartzke and Lindsay 2015), but even the utility of these operations is dubious because of the dynamics of cyber tools' coercive impact.

What is different about cyber tools is that the code or malware utilized in operations can be readily repurposed. There is extensive evidence of operations spreading beyond the initial attack zone which some even suggesting one of the most famous cyber operations (the Stuxnet attack against Iran) was repurposed to enemies of the U.S. for their own ends. A malicious group named Shadow Brokers released code supposedly developed by the US National Security Agency (NSA) and this code has been utilized by America's adversaries to attack the country that developed the code, such as North Korea's Wannacry ransomware campaign in 2017 (Mohurle and Patil 2017). This process is akin to literally turning an opposition missile right back at the attacker.

It is still early in the overall development of cyber operations and learning their optimal strategic utility. While the tool is not new, it is certainly not mature. Defenses and offenses still need to balance to meet the threat, artificial intelligence will pose another challenge to cyber operations making defenders more capable, and information operations in the cyber domain have led to widespread disinformation and political warfare. States with little concern for ethics, morals, and responsibility could utilize cyber operations for destructive purposes against

civilians, but these grand fears are unlikely to materialize. This brings us to our key question, has the character of war evolved with the onset of the cyber era?

The Evolving Character of War?

When studying war, every academic will inevitably come across Carl von Clausewitz's dictum on the nature and character of war (Clausewitz 1982). The nature of war can change slightly but it is wholly subordinate as an enterprise to the "original violence of its elements, hatred and animosity" (Clausewitz 1982: Chapter 1). The conditions of humanity mean for many that the essential components of violence and horror behind war will never change. The nature of war remains the same but the character of war can change because "from the character, the measures, the situation of the adversary, and the relations with which he is surrounded each side will draw conclusions by the law of probability as to the designs of the other, and act accordingly" (Clausewitz 1982: Chapter 1).

In short, the nature of war is dependent on the characteristics of humanity itself, but the character can change with the situation, the politics, technology, and the culture of moment. If those in control of the course of war sense a change in the opportunity for war because new technologies alter the landscape, the character of war has evitability changed. Almost directly tied to the concept of strategic culture (Snyder 1977, Johnston 1995), the course of strategy can be observed through behavior, but generally these behaviors do not change much through time.

The problem for those who promote a revolutionary view of cyber technology (Kello 2017) is that cyber tools have not changed the nature or character of war despite predictions to the contrary. Instead, cyber options only reinforce the patterns of old. States do not fight over technology but rather the traditional causes such as territorial issues (Valeriano and Maness 2015).

As we will discuss in this chapter, the coercive patterns of conflict, the dynamics of escalation, and the lust for total victory are not altered by cyber technologies. Instead, cyber operations just reinforce what has come before. As tools of the strong, cyber options serve to subjugate the weak. As tools of the weak, cyber options will cause disruption and serve notice to adversaries about capabilities, but they unlikely to alter the strategic balance of conflict and give the initiative to the weak.

The cyber conflicts of the now are result of the rivalries of the past, from the United States versus Russia (Maness and Valeriano 2015) to North Korea versus South Korea to even UAE versus Qatar (Valeriano, Maness et. al. 2017). Prior diplomatic failures and aggressions shape the cyber conflicts of the future. We have yet to see an international dispute caused solely by a cyber strategic action and are unlikely to witness such an event because the character of conflict has not changed with the advent of cyber conflict.

The case of Iran is illustrative of the typical dynamics of cyber conflict. There was an observed uptick in cyber actions by Iran after the United States pulled out of the nuclear agreement signed by President Obama (Joint Comprehensive Plan of Action 2015). Expressing dissatisfaction through cyber conflict is a typical outgrowth of cyber options, but Iran is not seeking to shape the behavior of its adversary through direct conflict because of the strength of the United States serves as a deterrent of sorts. Instead it responds with attacks against Saudi Arabia and its oil giant Aramco (once in 2012 in response to Stuxnet and again in 2019 in response to JCPOA and the War in Yemen, Baezner 2019).

The counter to this narrative is the constant Russian bombardment of cyber-related tactics in Ukraine, the supposed testing ground for future cyber operations (Greenberg 2019). The problem is there is no evidence that cyber operations against Ukraine, while it was directly

involved in a war with Russia, were out of the norm for a combat operation. The crucial question is if the use of cyber operations changes anything. For Kostyuk and Zhukov (2019), the answer is definitively "no" during the Ukraine-Russia war. Cyber operations did not change the flow of the battlefield and even seemingly devastating attacks such at the Not-Petya operation against Ukraine's financial services sector or the Estonia attacks in 2007 had a limited impact.

Taking a sobering look at the possibilities of digital technology is not meant to dismiss the possibilities of the future, rather it serves to remind that strategic calculations and the base politics of the past do not change with the fostering of new weapons leveraged to fight. Cyber operations and other modern technologies such as nuclear weapons might alter the bargaining patterns of states, but the patterns of conflict remain the same (cite nuclear chapter within). The pull of the past remains strong and the importance of this volume on the causes of war blends the past with the new to bring us to new understanding about the present.

There is No Cyber War

Despite many claims to the contrary (Kello 2013, Buchanan 2016, Kello 2017), cyber operations have not fundamentally revolutionized international relations. Instead, they have simply been added to the low end of coercive options (Nye 2017, Valeriano et. al. 2018) that states can utilize short of war to compel their adversaries to moderate behavior, and many of these options are information-related limiting physical destruction.

Thomas Rid was instrumental in pushing the field of cyber security quite early with the conjecture that cyber war will not take place (Rid 2012, Rid 2013). The main idea behind this statement was that death is unlikely to result from cyber war, in a pure definitional sense, war is unlikely. This does not mean that cyber conflict is unlikely, or rare, Rid was clear early on

suggesting that “cyber sabotage is easy” (Rid 2013) and goes further discussing the use of Russian active measures as a method of information warfare (Rid 2020).

At the same time, Valeriano and Maness (2012) started to advance the position through data and evidence that cyber conflict is a relatively underused tactic with limited ability to affect the battlefield. Cyberwar is an inflated threat incapable of changing the facts on the ground. They also demonstrate that Russia’s ability to cause mischief in international affairs is relatively toothless, since they depend on limited techniques such as cyber conflict. Even the U.S. presidential election hack of 2016 resulted in minimal success in changing voters’ minds about the candidates (Bail et. al. 2020).

The debate between Lindsay and Kello (2014) in the pages of *International Security* also pushed the field in new directions, placing scholars in corners with Lango (2016) labeling the divide as between cyber skeptics and cyber revolutionaries. Kello advances the revolutionary perspective suggesting context and content of international relations will change with cyber options being incorporated into national defense strategies (Lindsay and Kello 2014). Lindsay was skeptical of the potential of cyber factors to alter the international discourse and instead argued they would be added to the limited portfolio of options states can utilize during conflict, and perhaps more useful in times of peace and below the level of armed conflict (Lindsay and Kello 2014).

The reality is that a more moderate path needs to be carved out. Scholars are not skeptical of cyber operations, only skeptical of the dramatic proclamations of change and difference introduced by cyber options. Threat inflation dominates the field and news as cyber operations have been used sparingly so far, giving us limited examples of their utility. In the absence of evidence, base fears color the shape of the fear.

Gartzke and Lindsay's (2015) article on offense, defense, and deception was critical for the development of the field of cyber security. It pushes our aperture away from war and towards the idea that cyber conflict is primarily what might be called an intelligence game (Rovner 2019). Valeriano et. al. (2018) demonstrate empirically that the great majority of observed cyber conflicts are what might be categorized as espionage. The rise of cyber operations might coincide more with the evolution of espionage and other operations in the information environment rather than the evolution of war.

The perspective of restraint is critical for cyber security. Advanced by Valeriano and Maness (2015) who argue that restraint is the outcome we witness in cyber operations because of the limitations of the weapons, the vulnerability within each state, and general inability of the options to alter the cost-benefit calculus of the adversary. States will refrain from more harmful and damaging cyber operations using more low-level tools to keep the adversary confused and at bay.

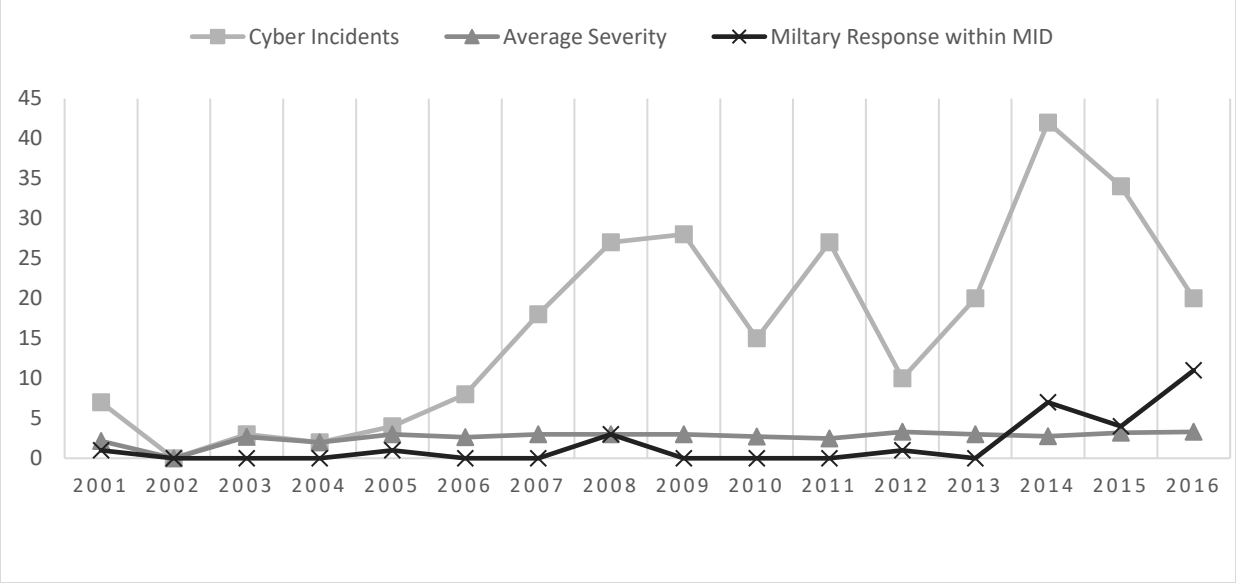
The stability-instability paradox introduced by Snyder (1965) has been instrumental is articulating a view that the instability that seems evident in cyberspace is stabilizing. "We should expect to see a lot more creative exploitation of global information infrastructure, but threat actors have strong incentives to restrain the intensity of their exploitation" (Lindsay and Gartzke 2016). Restraint can be seen an outcome of the limited coercive value of cyber operations, but it can also be a choice, or a strategy given the logical limitations of technology to provide an advantage to the attacker.

Figure 1 shows the number of cyber incidents over time, for the years 2000-2016. Data is extracted from the Dyadic Cyber Incident and Campaign Dataset (DCID), version 1.5 (Maness et. al. 2019). These data record all known state-initiated cyber incidents and campaigns between

rival states (Klein et. al. 2006) at the dyadic level. Incidents capture variables including method (vandalism, denial of service, network intrusions, network infiltrations), target type (private sector, civilian government, military government), strategic/coercive intent (disruption, short or long-term espionage/manipulation, degradations), presence of a following information operation (yes or no), and severity score (1-10, with a score of "1" being minor probing, to "10" being massive death as a result of a cyber operation), among others.[2]

Figure 1 shows that cyber incidents have been increasing over time but remaining around the same severity score through the duration of the 2000-2016 period. States have found cyber incidents useful for a foreign policy tactic but have yet to raise the stakes with more severe cyber operations that could lead to escalation. The stability-instability logic seems apparent in international cyber conflict.

Figure 1: State-initiated Cyber Incidents, Severity Average, Military Responses: 2000-2016



Source: Maness, Valeriano, and Jensen 2019.

[2] For a list and complete descriptions of the DCID variables, see https://drryanmaness.wixsite.com/cyberconflict.

Figure 1 also shows that military responses to cyber operations have been rare throughout the timeline, and only recently have military responses to cyber operations been on the rise. Data for military responses is compiled from three separate datasets, the Integrated Crisis Early Warning System (Boschee et. al. 2018), the Correlates of War (COW) Militarized International Dispute (Ghosn and Palmer 2003) dataset, and the International Crisis Behavior (Brecher and Wilkenfeld 1997) dataset. The "military usage" ICEWS variable is coded within a three-month (90 days) period after the cyber operation is either initiated (for non-espionage operations) or becomes public (most espionage variables). These variables are then overlaid with the MID variables (which only go to 2010) and the ICB variables (coded until 2015) to see if these military operations fall within the time period after the cyber operation.

Looking at Figure 1, we see that military responses uptick after the year 2013, likely due to the rise in organized violence seen globally in recent years. This includes the Russia-Ukraine protracted conflict, the Syrian civil war, and the rise of China's use of cyber operations within its disputes with regional rivals over issues regarding the South China Sea. Russia has been infiltrating Ukrainian networks in tandem with its other grey zone or "hybrid" tactics, such as disinformation operations and arming dissidents since the annexation of Crimea in 2014.

Distinct National Approaches to Cyber Conflict

The field of cyber security is dominated by conjecture because many suggest there is no way to collect data on cyber security events (Kello 2013). There are so many events that occur in a covert domain that it would be impossible to collect a representative sample of the data in the system. This challenge was met by Valeriano and Maness (2014, 2015) who demonstrate that collecting data on cyber operations between rival states is not only possible, but revelatory and necessary for progress in the field. Since then, others including the Council of Foreign Relations

and the University of Maryland's START program have collected on cyber events, but the DCID data (Maness et. al. 2019) represents the only peer-reviewed data set that also considers the issues of internal validity and externally reliability.

For too long, single examples have been leveraged to make large claims about the process of cyber conflict. Most of these examinations would not even meet the standards of a true case study, but instead represent surface-level explorations of an event to advance a specific predetermined position. Early and credible case studies in the field have been few and far between. Lindsay (2013) and Barzashka (2013) explore the Stuxnet operation in detail, demonstrating U.S. capability and intent in operations. While precision was the operative word that might describe the operation, Stuxnet likely had little overall effect on the ability of the Iranians to enrich uranium. Instead, to meet the challenge, Iran brought more centrifuges online and ended up enriching more uranium than before the attack.

Simple bivariate crosstabulations (crosstabs) are utilized in the tables below to uncover relationships between two or more categorical variables. Measuring Pearson residuals give us the key to where these significant relationships lie.[3] If the Pearson residual is above or below a score of two, statistical significance is present (at the 95 percent confidence level), where the utilization of a certain strategy or target type is found to be used more or less than what is expected, according to the normal distribution. In other words, if there is a positive significant relationship between variables (in bold and starred in the tables below), that indicates that the

[3] Pearson residuals measure the distance between an expected value of a crosstab analysis and the observed value by the number of standard deviations. If a Pearson residual has an absolute value of two (either more than 2 or less than -2), then we can infer that there is a statistically significant relationship between the two categorical variables for that specific cell. All significant relationships by cell in the following tables are in bold. All tables also have statistically significant chi-squared scores, indicating that all analyses to follow have significant relationships between the categorical variables and allows us to move forward with cell-specific Pearson residual tests.

preferred strategy, target type, or response is present. If there is a negative significant relationship between variables, it indicates that the preferred strategy, target type, or response is not present, and suggests that the other dependent variables are preferred over the significant negative highlighted variable.

Table 1 shows that the overall pattern of usage of cyber operations by the United States demonstrates a reliance of degrade operations that fit with the precision strike complex model of U.S. strategy (Valeriano et. al. 2018). The data demonstrate that the United States uses these operations sparingly, although only four of the total cells are statistically significant due to data limitations. Usually these degrade operations require intelligence collection, and several of the espionage incidents are precursors to the eventual operations utilized against rivals. The U.S. has not used a disruptive strategy in the dataset's current timeline, however in 2018 U.S. CYBERCOM launched a several days-long DDoS against Russia's Internet Research Agency (IRA), the famed troll farm cited by Special Counsel Robert Mueller's team in 2019 (Nakashima 2019).

Table 1: Crosstabs of Cyber Operations by strategy initiated by U.S. and its four major adversaries 2000-2016

Initiator		Disruption	Espionage	Degrade
United States	Count	**0**	10	**11**
	Expected Count	**5.47**	12.47	**3.07**
	Pearson residual	**-2.34****	-0.70	**4.53****
Russia	Count	19	35	11
	Expected Count	16.92	38.58	9.50
	Pearson residual	0.51	-0.58	0.49
Iran	Count	8	21	4
	Expected Count	8.60	19.60	4.82
	Pearson residual	-0.20	0.32	-0.37
China	Count	17	55	**2**
	Expected Count	19.26	43.93	**10.81**
	Pearson residual	-0.52	1.67	**-2.68****
North Korea	Count	**13**	9	4
	Expected Count	**6.77**	15.43	3.80
	Pearson residual	**2.40****	-1.64	0.10

****p<.05, n=219**
Pearson chi-squared (8) = 46.24 p=0.000**

On the other hand, China focuses mainly on espionage operations directed at gathering information and capability for future power projection. China's cyber strategy is more long-term, where the development of its technology and military sectors are important to its rise and quest for parity with the United States. China also uses disruptive strategies, which are usually against its regional rivals when conventional disputes manifest in the South China Sea over territory.

Russia is a revisionist power and is attempting to achieve the global perception that comes with being world power, and its specialized talent in cyber and disinformation campaigns is a big part of its foreign policy strategy. Russia typically utilizes espionage operations to enact cyber-enabled information operations against its rivals' domestic populations to sow discord and pursue its objectives more freely because of these disruptions. As Table 2 shows, Russia uses cyber operations against the private sector more than any other strategy when compared with the other four countries in the table, but these results are not statistically significant. Russia's strategy of staling technology and sensitive information feeds into its revisionist strategy in cyberspace to punch above their weight against richer or more powerful rivals.

Table 2: Crosstabs of Cyber Operations by target-type initiated by U.S. and its four major adversaries

Initiator		Private Sector	Govt non-military	Govt military
United States	Count	**2**	7	**12**
	Expected Count	**7.38**	10.07	**3.55**
	Pearson residual	**-1.98****	-0.97	**4.49****
Russia	Count	31	24	10
	Expected Count	22.85	31.16	10.98
	Pearson residual	1.70	-1.28	-0.30
Iran	Count	15	16	2
	Expected Count	11.60	15.82	5.58
	Pearson residual	1.00	0.05	-1.51

China	Count	17	**47**	10
	Expected Count	26.02	**35.48**	12.50
	Pearson residual	-1.77	**1.93****	-0.71
North Korea	Count	12	11	3
	Expected Count	9.14	12.47	4.39
	Pearson residual	0.95	-0.42	-0.66

****p<.05, n=219**

Pearson chi-squared (8) = 41.80 p=0.000**

China infiltrates civilian sectors of rival governments more than any other country, and this reinforces its attempts to steal sensitive information, intellectual property, and government secrets as it continues its long-term rise. The United States targets the military sectors of rival governments, in line with its attempted adherence to the Law of Armed Conflict (LOAC) and precision-strike mentality, where collateral damage is limited.

Overall, we know little of cyber capabilities. It is difficult to examine the overall spending in cyber security because most budgets are "black" or unknown. Understanding weapons stockpiles is an even more difficult process because malware stockpiles are unknown and there is an intense debate regarding state assets. There is even a likely a bigger challenge in the United States, with no overall coordination of malware or zero-day purchasing, US government organizations and allies may be in competition with themselves overall access to "cyber weapons."

Slayton (2017) makes the point that much of the capacity for cyber power comes from the talent and skill of individuals in the space. Craig and Valeriano (2016) apply the traditional study of arms races to cyber competition. While many in the space assume there are cyber arms races, this is an unknown at this point since we have little grasp at overall capabilities for most states. Some states like North and South Korea are likely engaged in a cyber arms race, but we have no idea on the overall scale of the problem internationally.

Table 3 lists power measures for the ten most active cyber states, according to DCID (Maness, et. al. 2019). Latent Cyber Capacity is a compilation of six World Bank measures under two categories: infrastructure and knowledge capital. The infrastructure category records World Bank scores recording broadband subscriptions per one thousand people, secure servers per one million people, and percentage of high-tech exports out of total manufactured exports (World Bank 2020). The knowledge capital category records scores from the World Bank that includes number of internet users per one thousand people, number of science, technology, engineering, and mathematical (STEM) journal articles published, and the number of patent applications for each country included in the DCID (World Bank 2020). These scores are then normalized and then averaged to get the power scores listed in Table 3.[4]

Table 3: Different Power Dynamics: Top Ten Most Active Cyber States

Country	**Latent Cyber Capacity (2016)**	**Economic Power (GDP billion $, 2019)**	**Military Power (Total billion $, 2019)**	**CINC (2012)**
United States	**6.82**	**20,490**	**750**	0.143291
China	6.43	13,400	237	**0.2181166**
S. Korea	6.22	1,531	44	0.0232826
Japan	5.86	4,970	49	0.0370358
Israel	5.32	351	20	0.0042498
Russia	5.03	1,578	48	0.0400789
Iran	4.53	440	19.6	0.0157625
India	4.35	2,597	61	0.0808987
Pakistan	4.11	305	11.4	0.0145536
N. Korea	4.01	40 (est.)	1.6	0.0132601

The United States is the top cyber power in the international system according to the latent cyber capacity index, followed by China and South Korea. The U.S. has a robust technology industry and a growing high-tech infrastructure backbone, as well as many patents, STEM publications, and research universities. China's kickstarted by espionage tech sector as

[4] For a more detailed description of the Latent Cyber Capability Index, see Valeriano et. al. (2018: Chapter 3).

well as its investment at modern infrastructure, and South Korea's homegrown tech sector put them near the top with the U.S. regarding these latent power scores. The rest of the columns show economic power measured in GDP per capita for 2019 (World Bank 2020), military expenditures per country (Global Firepower 2020), and the latest Composite Index of National Capability (CINC) scores for each country as of 2012 (Singer 1988).

Cyber Coercion and the Utility of Cyber Operations

In recent years, the question of cyber coercion has dominated the literature in the cyber conflict field. The reason why is not difficult to uncover, as coercion, or the ability of one state to influence the behavior of another, is the key question the field has generally ignored until recently. With many proclamations of the dramatic change brought on by cyber tools, few seemed to want to ask the basic question of how one would compel change with digital force? Answering the question of coercion directly impacts theories about the utility and effect of cyber operations, directly affecting the probability of war.

Coercion, under the construct advocated by Schelling (1980), can be divided into two forms, compellence and deterrence. Compellence is ability to make an actor behave in a manner they otherwise might not. While deterrence is active when an actor does not do what they otherwise might. Libicki (2016) was at the forefront is suggesting ways coercion may work in cyberspace, but few have sought to investigate the question from a social science perspective until more recently.

Borghard and Lonergan (2017) suggest that cyber power will have "limited effectiveness as a tool of coercion" because the cyber tools often lack clearly communicated threats, credibility, and reassurance. Valeriano et al. (2018) focus on the empirical dynamics of coercion in their monograph. They find that compellence is limited, resulting in a change in behavior only

five percent of the time. This rate is lower than most other forms of compellence that traditionally sit above 44 percent on average.

Some countries are better at coercion than others, for example the United States succeeds at a rate of 38 percent, mainly because they focus on the use of degrade campaigns which seek to change the behavior of the adversary. The United States also has the advantage of being the most powerful state in the system in terms of conventional capabilities, meaning it can back up its threats with action, ensuring compellent success more than usual.

Russia has been generally unsuccessful in leveraging cyber operations for effect. An examination conducted by Bail et. al. (2019) suggests that the Russian use of information operations only really reached those already supporting Donald Trump. Changing behavior is not evidenced here, if anything cyber-enabled information operations launched by Russia might have increased turnout and support for Trump, but the audience was ready to hear the message in the first place (Bail et. al. 2020). Kostyuk and Zhukov (2019) work is also instrumental in demonstrating the limits of Russian influence in cyberspace. During the war in Ukraine, no evidence of successful coercion could be identified by the scholars.

Deterrence is difficult to investigate empirically. Some suggest that the United States has deterred cyber conflict between adversaries above the threshold of armed conflict but failed below this zone. The challenge of course is that it is difficult to observe deterrence because successful deterrent moves will be unobserved, and successful deterrence entails non-action. More critically is the reality that states have not mobilized for deterrence under the conditions where most scholars would accept its application (Brantly 2018). For true deterrence, the state must have defenses to forestall attack in the first place, capabilities to respond, credibility to launch retaliatory attacks, and must also communicate what actions it wants to dissuade.

There is a possibility true deterrence can be implemented and tested in reality, but that would require a state to invoke real collaboration between the state and the private sector, ensuring that society overall is protected to forestall attacks in the first place. Layering deterrent principles in this way could increase the success of the construct, but once again we are left with a limited number of states with the ability to make this process work, suggesting the construct overall is limited.

The Cyberspace Solarium Commission (2020), in their comprehensive review of cyber policy and action, is advocating a policy of layered deterrence that mimics many of these stated panoplies (denial, cost imposition, credibility, entanglement, and a true public-private partnership). Achieving a whole-of-nation approach to cyber deterrence is critical, but also difficult to implement. Encoring coopering within the U.S. government is difficult enough, extending cooperation between government and private entities is orders of magnitude more complicated but also more critical given the tendency for the majority of targets to be in the private sector.

Escalation and Cyber Security

Escalation is defined as an increase in the nature or intensity of conflict, extending escalation theory to cyberspace would include situations in which "the target responds with more intense and costly cyber means (cyber escalation within the domain) or through breaching the cyber-kinetic threshold (cross-domain escalation)" (Borghard and Lonergan 2019). Libicki (2016) simplifies cyber escalation into two factors: intensity (striking deeper, lasting longer) or more extensive (striking new targets), plus adds the consideration that "attacks can jump from cyberspace to physical space."

Cyber escalation is then defined as a reaction with digital tools that increases intensity, aggression, or spreads the scope of conflict after an initial move in the digital domain. Theoretically, the cyber domain can contain escalation because of the uncertainty introduced by cyber weapons (Buchanan 2016). There is also the aspect of civilian punishment, attacks that hit what might be deemed civilian systems off limits, provoking escalation due to the violation in norms between two actors.

In practice, however, cyber escalation is rare. Stuxnet (2007-2010) is often cited as the prime example of cyber escalation, yet, put in the context of the wider dispute between the West and Iran over the development of nuclear weapons, the Stuxnet attack is actually a de-escalatory move because the other options on the table at the time were conventional strikes that would have caused death and destruction.

Talmadge (2019) makes the point that technology itself is rarely a sufficient condition for escalation, "cast[ing] doubt on the idea of emerging technologies as an independent, primary driver of otherwise avoidable escalation." Technology became the mask for the processes that enable escalation, rather than the cause of escalation itself. It is not the domain that produces escalation, but the action in domain that produces outcomes.

Empirically, we have ample evidence that escalation is limited in the cyber domain. Even in its simpler form, there is little retaliation, let alone escalation, in domain or even out of domain when cyber actions are the triggering events. When conflicts do escalate in cyberspace, we observe limited engagement between the parties unless there is already an outright war. As Valeriano et. al. (2018) note, "even when cyber exchanges between rivals escalate, they remain limited in scope outside of ongoing military conflict. That is, rivals may use cyber operations to probe the enemy, test their resolve, and signal the risks of significant escalation."

Data analysis supports these positions and is developed here from established data and taken from ongoing projects to support our background investigation into cyber escalation processes (Maness et. al. 2019) Table 5 shows the response patterns between the United States and its four major adversaries (Russia, Iran, China, North Korea) in the cyber domain, as well as how each country responds to a cyber-operation with a retaliatory cyber operation. Table 5 utilizes the cyber operation severity score from the DCID version 1.5 that measures the impact and national security importance of each state-initiated cyber operation between the years 2000-2016 between rival states (Maness et. al. 2019). The scale is interval and ranges from one to ten.

Table 5 shows that the United States is often on the receiving end of retaliation at a rate more than what is expected. However, these responses to U.S. cyber actions do not indicate within-domain escalation. The severity levels that were the response of "2" were retaliatory to U.S. actions that were of a higher severity level. Of the seven actions at the severity level of four, three represent a decrease in the initial attack severity and four represent an increase by one tick in severity. The only other country that witnesses a statistically significant level of retaliation at a greater rate than expected is Iran, which is wholly due to US or Israeli operations. China's significant negative relationship with severity score "2" shows that it prefers higher levels of severity when it retaliates in the cyber domain. Much of Chinese incidents involve entanglements with the United States, which is another great power with vast cyber capabilities. This propensity to use more severe attacks does not denote escalation, however. Escalation is rare in digital interactions as measured by rival states from 2000 to 2016.

Table 5: Crosstabs of Response Severity to Cyber Operations initiated by U.S. and its four major adversaries

Initiator		Response Severity						
		No Response	1	2	3	4	5	6
United States	Count	**7**	1	**5**	1	**7**	0	0
	Expected Count	**16.60**	0.10	**1.25**	0.96	**1.63**	0.39	0.10
	Pearson residual	**-2.35****	2.92	**3.36****	0.04	**4.21****	-0.62	-0.31
Russia	Count	52	0	6	5	1	1	0
	Expected Count	51.35	0.30	3.86	2.97	5.05	1.19	0.30
	Pearson residual	0.09	-0.55	1.09	1.18	-1.80	-0.17	-0.55
Iran	Count	27	0	0	**4**	1	1	0
	Expected Count	26.07	0.15	1.96	**1.51**	2.56	0.60	0.15
	Pearson residual	-0.20	-0.39	-1.40	**2.03****	-0.97	0.51	-0.39
China	Count	66	0	**0**	0	7	1	0
	Expected Count	58.46	0.34	**4.39**	3.38	5.74	1.35	0.34
	Pearson residual	0.99	-0.58	**-2.10****	-1.84	0.52	-0.30	-0.58
North Korea	Count	21	0	2	0	1	1	1
	Expected Count	20.54	0.12	1.54	1.19	2.012	0.48	0.12
	Pearson residual	0.10	-0.35	0.37	-1.09	-0.72	0.76	2.26

****p<.05, n=219**

Pearson chi-squared (24) = 76.50 p=0.000**

Table 6 shows how responses are related to the overall cyber strategy of the initiating states. In terms of response severity by strategic objective, disruptive efforts by initiating states are usually met with retaliatory disruptions, further indicating that the cyber domain is, for the most part, non-escalatory. Espionage campaigns are also commonly met with cyber operations that either steal or signal capabilities or displeasure for the originating action, but do not lead to a tit-for-tat escalatory ladder, as indicated in Table 2. Only occasionally do we see disruptions or espionage operations escalate to the severity level of "5," with this happening only five times over the 2000-2016 period.

Table 6: Crosstabs of Response Severity to Cyber Objectives

Cyber objective		Response Severity						
		No Response	1	2	3	4	5	6
Disruption	Count	58	0	**19**	4	2	3	0
	Expected Count	64.99	0.65	**8.73**	4.20	5.50	1.62	0.32
	Pearson residual	-0.87	-0.80	**3.48****	-0.10	-1.49	1.09	-0.57

Espionage	Count	118	1	**4**	8	12	2	0
	Expected Count	109.57	1.09	**14.72**	7.09	9.27	2.73	0.55
	Pearson residual	0.81	-0.09	**-2.79**	0.34	0.90	-0.44	-0.74
Degradation	Count	25	1	4	1	3	0	1
	Expected Count	26.45	0.26	3.55	1.71	2.24	0.66	0.13
	Pearson residual	-0.28	1.44	0.24	-0.54	0.51	-0.81	2.39

****p<.05, n=266**
Pearson chi-squared (12) = 36.49 p=0.000**

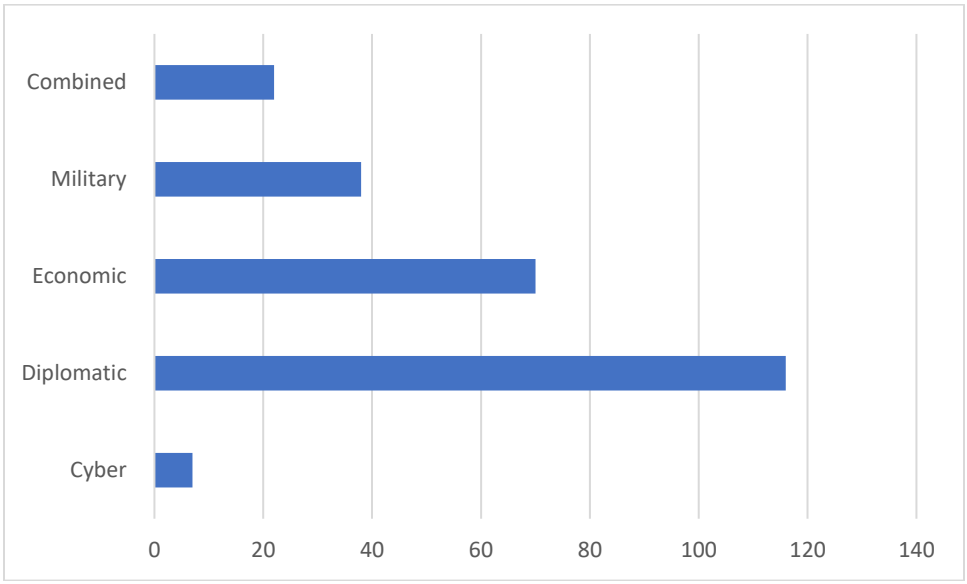
Results from wargames have demonstrated the complicated empirical picture of the escalation landscape in cyberspace (Schneider 2017). After examining war games from 2011 to 2016, Schneider finds that government officials were hesitant to use damaging cyber weapons. Most games only witness the use of cyber capabilities after the onset of conventional warfare, not before. For Jensen and Banks (2018), in the context of cyber options, escalation was the exception, not the norm.

To explore escalation when cyber options are present within the context of integrated options of national power, Jensen and Valeriano (2019) run a series of wargames on 259 participants including members of the military, students, and policymakers. The simulation situated participants in a typical crisis that was highly likely to escalate given a rivalry situation over an ongoing territorial dispute when the crises under examination was the third in a series over a five-year period.

The results demonstrate that escalation was not the norm. Based on a general baseline for all international conflict situations, most options fell below the 48 percent threshold. In fact, the only instance where escalation was the dominant option was when a cyber action started the crises and the target had no cyber response options. This suggests there are implications of attacking a state with cyber options when they do not have the ability to respond within domain. In most other situations, we witness few demands for escalation when cyber response options are on the table.

Overall, regardless of the situation, cyber escalation is usually not the dominant response. The reality is that even under dangerous conditions, cyber response options can actually moderate crisis response patterns. Surveys demonstrate there is a great amount of fear in the cyber domain, but this does not motivate overreaction (Gross et. al. 2017). Figure 2 shows the results from a cyber campaign directed dyads dataset. What is measured below is whether the combined cyber operation, which includes diplomatic, economic, and military variables extracted from ICEWS (Boschee et. al. 2018) have escalatory responses from the target from all four domains recorded in the campaigns. For a cyber response to be recorded, the target responds within one year from the start date of the original cyber operation from the initiator for disruptions and degradations, and from the date the operation becomes public for espionage operations. For a diplomatic response, the time frame is one month (30 days) after the cyber operation's initiation or public reporting, and for economic and military responses the time frame is three months (90 days) after the same criteria regarding the cyber operation. For cyber escalation, the severity score must go up at least one point regarding the cyber response. No cyber responses at the same severity score are included. For conventional responses, we use the Conflict and Mediation Event Observation (CAMEO) conflict-cooperation scores to measure escalation (Schrodt 2012). The CAMEO scale ranges from -10 to 10 where the more negative score, the more conflictual, and the more positive score the more cooperative the foreign policy action. If the conflict scores from each domain are lower (more negative) from the target state in retaliation for the cyber incident, escalation in each domain is recorded. The CAMEO scale ranges from -10 to 10 where the more negative score, the more conflictual, and the more positive score the more cooperative the foreign policy action.

Figure 2: Escalatory Responses per Domain: Cyber Campaigns



Source: Maness (2020).

Looking at Figure 2, we find that only seven cyber operations result in a higher cyber response in terms of DCID severity scores from the target state. This indicates that cyber does not beget more cyber, and it is extremely rare that a cyber operation is met with a more sophisticated and damaging operation from the original victim. Diplomatic escalation, where the diplomatic response is more severe than the initiating state's diplomatic action during the combined cyber campaign, is found in about one-third of all 266 campaigns recorded in DCID version 1.5. Economic escalation is found in 65 cyber campaigns, and this is a favorite response of the United States and its NATO partners on less powerful states who launch cyber campaigns against the Western powers. We see military escalation in nearly 40 cyber campaigns, and these are mostly embedded in ongoing conflicts in post-Soviet space, the Middle East, and the South China Sea. Finally, we see combined escalation, were the added totals of the diplomatic, economic, and military scores between the initiator and target, are at a higher overall CAMEO score.

Cyber as a Tool of Repression

Overall, the field has missed the boat on cyber war, there is no "war", but there is a strong probability that cyber tools can used to repress populations internally. Cyber weapons are better suited against the weak than the strong. Powerful states can fight back, and every state is vulnerable in cyberspace, even North Korea which has little dependence on the internet. Yet, individuals, activists, journals, and members of the civil society community have no great ability to fight back or protect themselves against a committed state adversary. The individual actor has little recourse when paired in a fight against a system of state control.

Some jump to the conclusion that cyber war will be fact of reality between states, but Arquilla and Rondfeldt (1996) early on suggested that netwar was a critical aspect of future cyber conflicts. Netwars would be fought between non-state or irregular forces, but the evolution of the domain will witness more conflicts between state and non-state actors morphing netwar into something different and unforeseen.

As Valeriano and Pytlak (2016) note "there has been a precipitous rise in malicious hacking, but it is not exhibited between states, rather it is from within them by governments seeking to maintain control over their populations. There is an increasing utilizing of cyber technology to silence dissent, often in direct contradiction with human rights law." This style of conflict can be termed "cyber repression", the use of digital tools by the state to repress, demean, and harass activists, journalists, and protectors within a state.

We can witness this effect by examining the pattern of internet shutdowns historically. Gohdes (2015) finds evidence that internet shutdowns coincide with wider state repression events, possibly increasing the ability of the state to control the population during times of turbulence. Gohdes (2015) notes "that governments have the strategic incentive to implement

internet blackouts in conjunction with larger repression operations against violence opposition forces." It not just that governments use internet shutdowns as a form of repression, but that governments can also use the access they provide to the internet to create a new style of targeted and precise repression (Gohdes 2020).

Instead of placing a fear of cyber war at the heart of upcoming interstate conflicts, its true place as likely a source of power by the state against adversaries during events of protest or rebellion. The utility of cyber weapons to control and subjugate a society are clear given the dependence many places on connectivity, add to this the rise of the surveillance state and there are the makings for something more dangerous than the proponents of cyberwar have ever dreamed. Limiting connectivity, repressing digital dissent, invading privacy, and surveilling domestic enemies are clear strategies for the state to prevail against internal adversaries and movements.

At the same time, capable individuals can marshal resources and capabilities to challenge the state digitally in response to increased repression. They can attack critical infrastructure, the media, and even the ballot box. A series of aggressive events by the state against a disaffected population is only likely to provoke that population to respond in kind. The car bombs of the future might be digital.

What We Know About Cyber War

For many, cyber war is the future. Warfare is a persistent reality while war is a condition that exemplifies the escalation of hostilities. The general decline of wars between states leads some to believe that this trend will only be a blimp in our history as new technologies reshape the global battlefield. The conjecture that future technologies will increase lethality has only met the devastating slap of reality.

The fear of the future shapes many visions of strategy, projecting a need to deal with an inflated threat now, before things get worse. This process has generally fed into the cult of the offensive (Snyder 1984) with many believing the best defense is a good offense in cyberspace. The challenge is that evidence paints a much different picture, despite visions of a future filled with cyber conflict, we instead find evidence cyber operations are limited as a coercive tool in international affairs. This is not to suggest that cyber operations will not be part of future battles, they will be adjunct and additive capabilities for all future fights. Cyber operations are not typically catalysts for war and may actually represent off-ramps away from war. Not all new capabilities need to be destabilizing, instead some technologies can increase the ability of states to signal displeasure and alter the course of conflicts.

Inherent in the analysis of cyber operations is the simple idea that cyber operations are not salient enough to spark wars. Too often, scholars of technology and security forget to ask a simple question, what are they fighting over (Diehl 1992)? Those that ignore the findings of the field of international relations are doomed to repeat the errors of the past and find cause for wars in things that are not critical enough to spark international conflagrations. With the constant rise in cyber operations every year, however, states must be seeing a strategic utility to these options. Most cyber operations are usually below the threshold of armed conflict and can perhaps be considered a new type of political warfare, which is "the logical application of Clausewitz's doctrine in times of peace" (Kennan 1948). States will try to gain bargaining advantages with their adversaries using digital tools in order to project power and cause asymmetries.

On the other hand, conflict processes scholars often fail to examine the strategic logic of their positions. If there is no inherent logic for the coercive power of a strategy, there is a dubious connection between that strategy, technology or means of warfare and the onset of war

itself. Technologies like cyber options, nuclear weapons, chemical weapons are not reshaping the character of war, instead they are altering the bargaining landscape below the threshold for the use of force. This alteration of the international conflict landscape has not been noticed by the field at large. Moving forward, the field of conflict studies needs to be aware of the evolution of the conflict landscape and reality of how emergent technologies reshape the perceptions of conflict. Cyber conflict is in our future, but cyber war will not come.

References

Arquilla, John, and David Ronfeldt. "The advent of netwar (revisited)." *Networks and netwars: The future of terror, crime, and militancy* (2001): 1-25.

Baezner, Marie. *Iranian Cyber-activities in the Context of Regional Rivalries and International Tensions*. ETH Zurich, 2019.

Bail, Christopher A., Brian Guay, Emily Maloney, Aidan Combs, D. Sunshine Hillygus, Friedolin Merhout, Deen Freelon, and Alexander Volfovsky. "Assessing the Russian Internet Research Agency's impact on the political attitudes and behaviors of American Twitter users in late 2017." *Proceedings of the national academy of sciences* 117, no. 1 (2020): 243-250.

Barzashka, Ivanka. "Are Cyber-Weapons Effective? Assessing Stuxnet's Impact on the Iranian Enrichment Programme." *The RUSI Journal* 158, no. 2 (2013): 48-56.

Borghard, Erica D., and Shawn W. Lonergan. "Cyber operations as imperfect tools of escalation." *Strategic Studies Quarterly* 13, no. 3 (2019): 122-145.

Boschee, Elizabeth, Jennifer Lautenschlager, Sean O'Brien, Steve Shellman, and James Starz. "ICEWS automated daily event data." *Harvard Dataverse* (2018).

Brantly, Aaron F. "The cyber deterrence problem." In *2018 10th International Conference on Cyber Conflict (CyCon)*, pp. 31-54. IEEE, 2018.

Brecher, Michael, and Jonathan Wilkenfeld. *A study of crisis*. University of Michigan Press, 1997.

Buchanan, Ben. *The cybersecurity dilemma: Hacking, trust, and fear between nations*. Oxford University Press, 2016.

Clarke, Richard Alan, and Robert K. Knake. *Cyber war*. Old Saybrook: Tantor Media, Incorporated, 2014.

Clausewitz, Carl. *On war*. Vol. 20. Penguin UK, 1982.

Craig, Anthony, and Brandon Valeriano. "Conceptualising cyber arms races." In *2016 8th International Conference on Cyber Conflict (CyCon)*, pp. 141-158. IEEE, 2016.

Cyberspace Solarium Commission Report. 2020. Available at: https://www.solarium.gov/

Diehl, Paul F. "What are they fighting for? The importance of issues in international conflict research." *Journal of Peace Research* 29, no. 3 (1992): 333-344.

Dykstra, John, Glen A. Larson, Richard A. Colla, Alan J. Levi, Richard Hatch, Dirk Benedict, Lorne Greene, et al. 2003. *Battlestar Galactica*. Universal City, CA: Universal.

Gartzke, Erik. "The myth of cyberwar: bringing war in cyberspace back down to earth." *International Security* 38, no. 2 (2013): 41-73.

Gartzke, Erik, and Jon R. Lindsay. "Weaving tangled webs: offense, defense, and deception in cyberspace." *Security Studies* 24, no. 2 (2015): 316-348.

Ghosn, Faten, and Glenn Palmer. "Militarized interstate dispute data, version 3.0." (2003).

Gohdes, Anita R. "Pulling the plug: Network disruptions and violence in civil conflict." *Journal of Peace Research* 52, no. 3 (2015): 352-367.

Gohdes, Anita R. "Repression technology: Internet accessibility and state violence." *American Journal of Political Science* (2020).

Greenberg, Andy. *Sandworm: A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, 2019.

Gross, Michael L., Daphna Canetti, and Dana R. Vashdi. "Cyberterrorism: its effects on psychological well-being, public confidence and political attitudes." *Journal of Cybersecurity* 3, no. 1 (2017): 49-58.

Jensen, Benjamin, and David Banks. *Cyber Operations in Conflict: Lessons from Analytic Wargames*. Center for Long-Term Cybersecurity, UC Berkeley, 2018.

Jensen, Benjamin, and Brandon Valeriano. "Cyber Escalation Dynamics: Results from War Game Experiments International Studies Association, Annual Meeting Panel: War Gaming and Simulations in International Conflict March 27, 2019." (2019).

Johnston, Alastair Iain. "Thinking about strategic culture." *International security* 19, no. 4 (1995): 32-64.

Joint Comprehensive Plan of Action, U.S. Treasury, available at: https://www.treasury.gov/resource-center/sanctions/Programs/Pages/jpoa_archive.aspx

Kaplan, Fred. *Dark territory: The secret history of cyber war*. Simon and Schuster, 2016.

Kello, Lucas. "The meaning of the cyber revolution: Perils to theory and statecraft." *International Security* 38, no. 2 (2013): 7-40.

Kello, Lucas. *The virtual weapon and international order*. Yale University Press, 2017.

Kennan, George. "The inauguration of organized political warfare." *State Department Policy Planning Staff, National Archives and Records Administration, RG* 273 (1948).

Klein, James P., Gary Goertz, and Paul F. Diehl. "The new rivalry dataset: Procedures and patterns." *Journal of Peace Research* 43, no. 3 (2006): 331-348.

Kostyuk, Nadiya, and Yuri M. Zhukov. "Invisible digital front: Can cyber attacks shape battlefield events?." *Journal of Conflict Resolution* 63, no. 2 (2019): 317-347.

Langø, Hans-Inge. "Competing academic approaches to cyber security." In *Conflict in Cyber Space*, pp. 23-42. Routledge, 2016.

Libicki, Martin. *Cyberspace in peace and war*. Naval Institute Press, 2016.

Lindsay, Jon R. "Stuxnet and the limits of cyber warfare." *Security Studies* 22, no. 3 (2013): 365-404.

Lindsay, Jon R., and Lucas Kello. "Correspondence: a cyber disagreement." *International Security* 39, no. 2 (2014): 181-192.

Lindsay, Jon R., and Erik Gartzke. "Coercion through cyberspace: the stability-instability paradox revisited." *The Power to Hurt: Coercion in Theory and in Practice* (2016): 176-204.

Maness, Ryan, and Brandon Valeriano. *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*. Springer, 2015.

Maness, Ryan C., Brandon Valeriano, and Benjamin Jensen. “The Dyadic Cyber Incident and Campaign Dataset (DCID), version 1.5, 2019. Available at: https://drryanmaness.wixsite.com/cyberconflict/cyber-conflict-dataset

Maness, Ryan C. “Directed Dyads addendum to DCID version 1.5”, working dataset, 2020.

Mohurle, Savita, and Manisha Patil. "A brief study of wannacry threat: Ransomware attack 2017." *International Journal of Advanced Research in Computer Science* 8, no. 5 (2017).

Nakashima, Ellen. “U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms,” *The Washington Post*, 2/27/2019, accessed 7/27/2020, available at: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Nye Jr, Joseph S. "Deterrence and dissuasion in cyberspace." *International security* 41, no. 3 (2017): 44-71.

Ranking, Military Strength. "Global Firepower Index [Electronic resource]. 2019." *URL: https://www. globalfirepower. com/countries-listing. asp (accessed: 28.11. 2019)*.

Rid, Thomas. "Cyber war will not take place." *Journal of strategic studies* 35, no. 1 (2012): 5-32.

Rid, Thomas. *Cyber war will not take place*. Oxford University Press, USA, 2013.

Rid, Thomas. *Active Measures: The Secret History of Disinformation and Political Warfare*. Farrar, Straus and Giroux, 2020.

Rovner, Joshua. "Cyber War as an Intelligence Contest." *War on the Rocks* 16 (2019).

Schelling, Thomas C. *The strategy of conflict*. Harvard university press, 1980.

Schneider, Jacquelyn. "Cyber and crisis escalation: insights from wargaming." In *USASOC Futures Forum*. 2017.

Schrodt, Philip A. "Cameo: Conflict and mediation event observations event and actor codebook." *Pennsylvania State University* (2012).

Singer, Peter Warren, and August Cole. *Ghost fleet: A novel of the next World War*. Houghton Mifflin Harcourt, 2015.

Singer, Joel David, and Melvin Small. *The wages of war, 1816-1965: a statistical handbook*. John Wiley & Sons, 1972.

Singer, J. David. "Reconstructing the correlates of war dataset on material capabilities of states, 1816–1985." *International Interactions* 14, no. 2 (1988): 115-132.

Slayton, Rebecca. "What is the cyber offense-defense balance? Conceptions, causes, and assessment." *International Security* 41, no. 3 (2017): 72-109.

Snyder, Glenn Herald. *The balance of power and the balance of terror*. San Francisco: Chandler, 1965.

Snyder, Jack L. *The soviet strategic culture*. 1977.

Snyder, Jack. "Civil-Military Relations and the Cult of the Offensive, 1914 and 1984." *International Security* 9, no. 1 (1984): 108-146.

Talmadge, Caitlin. "Emerging technology and intra-war escalation risks: Evidence from the Cold War, implications for today." *Journal of Strategic Studies* 42, no. 6 (2019): 864-887.

Valeriano, Brandon, and Ryan C. Maness. "Persistent enemies and cybersecurity: the future of rivalry in an age of information warfare." In Derek Reveron (Ed.) *Cyberspace and National Security* (2012, Goergetown): 139-158.

Valeriano, Brandon, and Ryan C. Maness. "The dynamics of cyber conflict between rival antagonists, 2001–11." *Journal of Peace Research* 51, no. 3 (2014): 347-360.

Valeriano, Brandon, and Ryan C. Maness. *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press, USA, 2015.

Valeriano, Brandon, Ryan C. Maness, and Benjamin Jensen. "Cyberwarfare Has Taken a New Turn: Yes, It's Time to Worry." *Washington Post: The Monkey Cage* 7, no. 13 (2017): 2017.

Valeriano, Brandon, Benjamin M. Jensen, and Ryan C. Maness. *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press, 2018.

Valeriano, Brandon, and Allison Pytlak. "Closing the Internet up: The rise of cyber repression." *Council on Foreign Relations Net Politics* (2016).

Wargames. Film. United States : MGM, 1983.

World Bank Databank, accessed 7/27/2020, available at: https://databank.worldbank.org/home.aspx