Factors That Motivate State-Sponsored Cyberattacks

Lance Y. Hunter, Ph.D.
Craig Douglas Albert, Ph.D.
Eric Garrett

ABSTRACT

The study of the factors involved in the initiation of violent interstate conflicts has been well documented within international relations. However, scholars have yet to analyze the factors associated with the initiation of international state-sponsored cyberattacks due to the lack of available data. This study is a first attempt to address this limitation. This project examines the political, economic, and military factors associated with the initiation of state-sponsored cyberattacks from 2005–2012, using a unique dataset that incorporates author-collected political, economic, and military data, along with cyber data on known state-sponsored cyberattacks extracted from the Council on Foreign Relations (CFR) Cyber Operations Tracker Dataset. With this unique dataset, we seek to better understand those states most likely to cyberattack other states.

INTRODUCTION

Cyber conflict is an emerging topic within the field of international relations. Every nation has been affected in some form by illegal cyber operations deployed by other nations or groups.[1] Sixty percent of senior internet technology officials predict that the severity of nation-state attacks against governments and corporations will continue to increase over time and even lead to all out cyber-war.[2] Observers note: "In the future, wars will not be fought by guns or with planes that drop bombs. They will also be fought with the click of a mouse a half a world away that unleashes carefully weaponized computer programs that disrupt or destroy critical industries like utilities, transportation, communications and energy."[3] Scholars such as Kello contend: "[t]he implications for international security are potentially serious: according to [calculated ambiguity], a

Lance Y. Hunter, Ph.D., is an Associate Professor of International Relations at Augusta University. His research focuses on how terrorist attacks influence politics in democratic countries and how political decisions within countries affect conflicts worldwide. His work has appeared in journals such as: *Journal of Peace Research, Terrorism and Political Violence, Party Politics, Studies in Conflict and Terrorism, Armed Forces and Society, Conflict, Security and Development, European Political Science, and Global Policy*.

cyber event can occur that does not meet the traditional definition of war but nevertheless elicits a reprisal of commensurate severity."[4]

While the threat of cyberconflict is ever-present, the systematic study of the factors involved in the initiation of state-sponsored cyberconflict is in its infancy stages. Factors that lead to military conflicts between nation-states has been exhaustively researched, but far less is known about the factors that precipitate cyberconflicts cross-nationally. Relatively speaking, this project is therefore one of earlier attempts to examine the political, economic, and military factors associated with the initiation of state sponsored cyberattacks, and focuses on the years 2005-12. Our dataset includes political, economic, and military data on 143 states, and on known state-sponsored cyberattacks collected from the Council on Foreign Relations (CFR) Cyber Operations Tracker Dataset (COTD). In analyzing this unique dataset, we attempt to better understand what states are more or less likely to cyberattack other states.

Here, we seek to identify those variables most important in influencing which states are most likely to initiate cyberattacks, and factors that would influence the frequency of such cyberattacks. We also include a complementary descriptive analysis of factors associated with cyberattacks by analyzing the political, economic, and military features of cyberattacking states as compared to cyberattack victim states. This descriptive analysis complements our statistical analysis to better understand the factors key to motivating state-sponsored cyberattacks. The descriptive analysis is from 2005-16.

We first examine the factors traditionally associated with military conflict between states, and then turn to how, per existing literature, such factors themselves may influence cyberconflict. We next proceed to empirical analysis, discussing first our statistical analysis and results, followed by our descriptive analysis and findings. Lastly, we present our conclusions and their implications.

Craig Douglas Albert, Ph.D., is an Associate Professor of Political Science and the Graduate Director of the Master of Arts in Intelligence and Security Studies at Augusta University, with concentrations focused on international relations, ethnic conflict, cyberterrorism and cyberwar, and the scholarship of teaching and learning. He is widely published, including articles in the *Journal of Political Science Education; Iran and the Caucasus; Politics; East European Politics; Chicago-Kent Law Review; Middle Grades Review; The Journal of International Social Studies*. Dr. Albert testified before the U.S. Congress' joint subcommittee of the House Foreign Affairs Committee concerning the Boston Bombings. You can follow him on social media @DrCraigDAlbert.

Power

A large body of research within international relations links economic and military power to the initiation of military conflicts, as more powerful states tend to have a greater number of interests to protect so are more likely to initiate military conflicts in the protection of those geopolitical interests.[5] Thus, an appropriate question to ask is, does economic and military power similarly affect the initiation of cyberconflicts?

Many scholars consider cyberpower as equal to military power projection in the physical domain and should be conceptualized and studied similarly.[6] As such, power allows an actor to dominate other states leading the more powerful state to achieve one's interests.[7] Additionally, it can be argued that deploying offensive cyber capabilities is less effective in projecting power than traditional kinetic military weapons because the lesser chance of palpably injuring the enemy, especially from an unsophisticated cyberattack such as a Computer Network Attack (CNA).[8] A sophisticated cyberattack however, could yield more force projection or damage depending on the scope of the attack. Conversely, executing such an attack requires a substantial reserve of power projection capability because such an attack requires strength in technological sophistication, skill, ingenuity, reconnaissance, social engineering and sophisticated knowledge of network vulnerabilities.[9] In other words, cyber capability is a corollary of relative power generally. However, one cannot rest assured on the strategy of deterrence to work in cyberspace. Offense holds the competitive advantage concerning the cyber offense-defense balance as, due to the difficulty of attribution, deterrence can be undermined. As Lindsay notes, "weaker actors can attack the control systems of superior adversaries to achieve levels of physical disruption possible previously only through kinetic bombing."[10] Thus, one could argue that weaker powers are more prone to be cyber-attackers than great powers.

Eric Garrett is a recent graduate of Augusta University's Master of Arts in Intelligence and Security Studies program, holds numerous professional cybersecurity certifications in penetration testing, incident response, host and network forensics, and network and systems security monitoring.

But the flip side of this argument must also be considered. First is the fact that the flexible nature of cyber weapons render them vulnerable to be "captured, manipulated, and turned against their creators".[11] Also, the first-mover advantage might be more modest in the cyber domain if attacks are mitigated or otherwise rendered ineffective by a victim who responds at will, possibly even using a variant of the weapon of its attacker. If hiding the cyber weapon is key to its efficacy, offensive dominance can be easily neutralized by premature disclosure of capabilities. Asymmetric effects may only be present as disproportionate costs as weaker states can attempt to rebalance an asymmetric relationship with a more powerful state by using inexpensive tools and methods to inflict heavy victim expenses on the targeted state. Yet success of this strategy may be offset by limitations inherent to the first mover's cyber domain advantage.

Some experts explain that cyberattacks that fall short of qualifying as a coercive tool, may nevertheless be expressions of brute force as a "means of forcible accomplishments."[12] Cyber operations are also considered well-suited as an asymmetric warfare component that complements rather than replaces conventional operations. A cyber-plus attack describes a scenario where a computer network attack is used as a non-violent precursor to other actions to achieve direct political or military objectives.[13] Rather than achieving a one-and-done attack or a cyber–Pearl Harbor, this could maximize conventional effects and also reduce the risk of play-back of the cyber weapons against their creators, or other collateral damage. Mazanec points to Russian cyberattacks used against the Georgian government and command and control networks as a progression of cyber tools being used "as a force multiplier to conventional military operations" causing "tangible disruption and effects beyond CNE [computer network exploitation]-style espionage."[14] Furthermore, these otherwise

unsophisticated attacks were ineffective unless focused on interfering with the Georgian government's ability to communicate by denying, degrading, and disrupting command and control systems.[15]

Cyberattacks facilitate the use of non-violent means to achieve interests, whether by militarized effects or through sabotage. Complicating validation of their impact as a means of power projection is that cyberattacks generally are better suited for stealthy actions that may remain secret in both their capabilities, use, and effects.[16] On the other hand, cyber tools used can equate to cyber tools lost, potentially giving defensive postures an advantage as costly cyber tools have a limited time in which they can reveal defensive vulnerabilities and illuminate system weaknesses that can be repaired. This also reduces the ability for coercion as the more offensive a deployed tool is, the less credibility it has when defensive postures are adjusted to defeat the exploits. A defensive mindset benefiting from greater awareness of vulnerabilities and weaknesses also drives up the costs and required level of sophistication to preserve offensive cyber weapons effectiveness.

Complicating the issue is that cyberpower, like other forms of power, can be used as hard power (i.e., a Critical Infrastructure Systems attack) or soft power through information warfare or social media weaponization designed for intelligence operations.[17] As to weaker states, even if a regime has major cyber capabilities, if it lacks corresponding economic and/or military prowess, it may refrain from carrying out cyberattacks for fear of kinetic response. Executing a cyberattack would be too costly to risk conflict escalation and spillover effects from cyberspace to physical territory. But smaller states that can effectively carry out a sophisticated and undetectable cyberattack may view the rewards as outweighing the costs, and act more offensively in the cyber realm. As Gartzke and Lindsay write, "Cyber operations alone lack the insurance policy of hard military power, so their success depends on the success of deception."[18] However, cyberattacks will seldom go unnoticed, particularly if attribution is intended and necessary to demonstrate power, so the balance between weaker and stronger states could rely on the known threat of disproportionate costs and the need to back up fragile capabilities with hard military power.[19] This could form a basis of deterrence based on restraint derived from risk assessment and by considering the complementary threats and vulnerabilities of both adversary and friendly systems.

Based on the information discussed above, we present two competing hypotheses regarding the impact of power on the initiation of state-sponsored cyberattacks. The first hypothesis is that states with greater power are more likely to initiate cyberattacks due to their power advantage, which would correspond to literature on power and military conflict that finds more powerful states are more likely to initiate military disputes.

- **Hypothesis 1:** More powerful states (i.e., states with greater economic and military power) are more likely to initiate cyberattacks than weaker states.

Our second hypothesis is in respect to the notion that state-sponsored cyberattacks are often a tool used by weaker states due to the possibility of deception and the potential need for less resources (economic and military) to execute a cyberattack compared with more traditional forms of conflict.

- **Hypothesis 2:** Less powerful states (i.e., states with less economic and military power) are more likely to initiate cyberattacks than powerful states.

We now turn to examining the literature pertaining to regime type and conflict.

Regime Type

Many researchers have investigated the relationship between regime type and military conflict. This area of research has considered how the presence or absence of democratic institutions affects conflict. While research has largely confirmed that democracies generally have peaceful relations with each other,[20] another strand of research has investigated the extent that regime type influences conflict in general,[21] though this line of research has produced mixed results. Some research has found that democracies are as equally conflict prone as authoritarian states[22] while other research has found that the level and type of democratic institutions within states can have pacifying effects on the likelihood of conflict.[23] Lastly, other scholars have found that democratic and authoritarian states select into different types of conflicts due to their disparate political institutions.[24]

While exhaustive research exists in regards to the relationship between democratization and war and the correlation between democratic regimes and peace, research examining the impact of regime type on cyberspace and how regime type influences the initiation of cyberattacks is quite limited. Yet it is reasonable to assume that states with more aggressive domestic exploitation of cyberspace are likely to have the same framework when considering cyber foreign policy. For instance, MacKinnon argues that although many hoped, especially in the technology corporate sector, that the internet would help democratize and open spaces within authoritarian regimes, cyberspace has actually had the opposite effect.[25] MacKinnon calls this new regime space, networked authoritarianism, where the government controls netizens through internet capabilities.[26] The author alarmingly notes that, "[s]trong governments in weak or new democracies are using second-and third-generation Internet controls in ways that contribute to the erosion of democracy and slippage back toward authoritarianism."[27] Stateless packet inspection, falling into the category of first-generation Internet controls, includes simple filtering methods based on metadata found within traffic headers such as machine addresses or ports and protocols. In contrast, second and third-generation Internet controls apply increasingly complex algorithms based on higher levels of traffic content, through stateful or deep packet inspection, to shape or deny traffic while maintaining awareness of context. More advanced Internet controls falling under the next-generation label increasingly seek to apply machine learning and artificial intelligence concepts to increase data tracking and awareness.[28]

These controls may also lead to establishing behavioral norms, compliance, and imposing rules rather than hardware and software operations.[29] With increased capabilities to examine Internet traffic, next-generation controls also collide with privacy and governance issues.

Deibert notes that authoritarian regimes are actually shaping cyberspace to their own strategic advantage, utilizing technological, legal, extralegal, and other target information controls.[30] Generally, these measures have had "the effect of strengthening the state at the expense of human rights and civil society."[31] Most relevant to the present paper is Deibert's analysis of third-generation controls, which are active offensive measures involving surveillance, targeted espionage, and other methods of covert disruptions in cyberspace.[32] These third-generation controls target human-rights, prodemocracy, and independent movements outside the state in which the controls are launched.[33]

Dr. Jan Kallberg argues that cyberattacks work best, according to strategic cyberwar theory against weak regimes or, "the theory's predictive power is strongest when applied to targeting theocracies, authoritarian regimes, and dysfunctional experimental democracies, because the common tenet is weak institutions."[34] Kallberg further notes that fully functioning democracies have a strategic advantage in cyberwar because of their institutional stability and accepted institutions.[35] Thus, it is reasonable to assume that democracies will not engage in cyberwarfare against one another, but are likely to engage in cyberconflict against non-democracies, or anocracies (i.e., hybrid regimes). Kallberg explains that "[a]n attack will fail to destabilize the targeted society if the institutions are intact after the attack....Therefore it is important to ensure that the attack is of the magnitude that it pushes the targeted society over the threshold to entropy."[36]

Based on the existing literature, we present two additional competing hypotheses regarding the relationship between regime type and the initiation of cyberattacks. The third hypothesis engages with the notion that democratic states should be less likely to initiate cyberattacks due to their domestic norms and membership in specific types of international institutions that encourage more cooperative behavior in foreign policy. This hypothesis aligns with literature that finds democratic states are more dovish compared with authoritarian regimes due to their domestic norms, which may be transferred to the international arena, along with their membership in specific international institutions that serve to moderate aggressive foreign policy behavior and promote cooperation.

- **Hypothesis 3:** Democratic states are less likely to initiate cyberattacks than authoritarian states.

An opposing hypothesis is that democratic states may be more likely to initiate cyberattacks as cyberattacks could be an alternative tool to actual military engagement. This proposition views democracies as more likely to advance cyberattacks because they are the less costly alternative to traditional military conflict.

- **Hypothesis 4:** Democratic states are more likely to initiate cyberattacks than authoritarian states.

Research Design: Statistical Analysis

To test our hypotheses, we include include data on 143 countries from 2005-12 (all data that is available) in our statistical analysis of the relationship among state power, regime type, and the initiation of cyberattacks. The cyberattack data are taken from the Council on Foreign Relations (CFR) Cyber Operations Tracker Dataset (COTD),[37] and includes data on cyberattacks that occurred during that time. The state-sponsored cyber activities included are as follows: "The data exclusively tracks incidents and threat actors engaged in denial-of-service attacks, espionage, defacement, destruction of data, sabotage, and doxing."[38] One limitation in the dataset, which exists in all cyberconflict datasets, is not all cyberattacks that occurred during the time period are included due to limited information as to the full universe of cyberattacks that transpired during the time span. Thus, the attacks included in the CFR COTD pertain to verified attacks where information was largely known regarding both the attacker and the targeted victim states. The primary dependent variable from the CFR COTD we generate is the measure Cyberattack Count. The Cyberattack count variable captures the number of cyberattacks initiated by a given state for the year observed.

State Power

To measure the level of power for each state we use the Composite Index of National Capabilities (CINC) measure taken from the Correlates of War Dataset,[39] which is one of the most widely used measures of state power in international relations.[40] The CINC score gauges the level of power each state has relative to all other states, and is generated by calculating a state's total score based on six core components: iron and steel production (thousands of tons), military expenditures, military personnel, energy consumption, total population (thousands) and urban population. CINC score increases for any state indicates an increase in power relative to all other states, and is measured on a continuous 0 to 1 scale.[41]

Regime Type

The primary measure we use to assess whether a state is democratic or authoritarian is the widely recognized Polity2 measure for the Polity IV Database.[42] The Polity2 measure is widely used in international relations and is considered to be a valid and reliable measure of regime type.[43] The Polity2 measure captures the level of democracy or authoritarianism within states and ranges from -10 to 10. Higher values indicate a state is more democratic. Lower values indicate a state is more authoritarian. Political rights and civil liberties are two additional variables that are related to regime type included in our analysis. Political rights and civil liberties capture different aspects of the nature of governance within states that differ from what Polity2 measures. We use the political rights and civil liberties measures from the Freedom House

database to capture the extent that political rights and civil liberties of each states.[44] Political rights measure one's freedom to participate in the political process by voting for elected leaders in free and fair elections, running for political office, and joining political organizations. The political rights measure is coded on an ordinal seven-point scale. The higher to value (here, 7) the lower political rights, with (1) depicting the widest possible range of political rights. The civil liberties measure gages one's right to openly express political beliefs, or belong to political and civil organizations, or have personal privacy and autonomy protected, and the rule of law. The civil liberties measure is coded on the same ordinal seven-point scale described above, with the lower value being the greatest civil liberties. The highest value (7) indicates a state has few or no civil liberties, and (1) indicates a state enjoys a wide range of civil liberties. Thus, higher values equate to a state having fewer civil liberties.

Control Variables

Our statistical analysis includes the variables discussed above, along with a number of other variables traditionally used to explain conflict initiation in order to attempt to identify those factors more closely associated with initiation of cyberattacks. These measures include economic variables that past studies often link to conflict (Inflation and Trade).[45] To control for the effects of any potential ongoing conflicts on the initiation of cyberattacks we also include another standard measure in conflict/terrorism literature, i.e., the number of battlefield deaths within a state for any given year, both military and civilian. The data for the three variables (Inflation, Trade, Battlefield Deaths) are from the World Development Indicators.[46]

Estimation Procedure

We conducted a cross-national time series analysis that examines how our economic and political variables influence the initiation of state-sponsored cyberattacks. For our primary measure, Cyberattack Count, we employ a random effect, time-series regression with a lagged dependent variable to control for autocorrelation. We used this estimation procedure based on the nature of our data, and since we are interested in the between-state variation in our sample. Our unit of analysis is state year.

Results

Table 1 (Model 1) displays the results that includes Cyberattack Count as the dependent variable. The CINC measure proved to have a positive and statistically significant relationship with the Cyberattack Count dependent variable.[47] Thus, an increase in CINC score corresponds to a statistically significant greater number of cyberattacks. None of the other remaining political and economic variables reflected statistical significance in our models. Thus, state power appears to be the most influential factor regarding cyberattack initiation.

When examining the real-world implications of state power (CINC Score) on the number of cyberattacks initiated by states it is important to examine the predictive margins pertaining to state power's effect on cyberattack initiation. The predictive margins indicate the effects changes in the primary independent variable (CINC Score) have on the dependent variable when all other variables are held constant at their mean values. In Table 2 (Model 2), and Figure (1), we observe the expected number of initiated cyberattacks based on changes in levels of relative power as the CINC measure increases in increments of .10 (i.e., an increase in 10% relative power). When analyzing the predictive margins, we observe that when the CINC score is at the minimum level of relative power (0) the expected number of cyberattacks initiated is .0025, and when the CINC Score is at the maximum level of relative power (1) the expected number of cyberattacks initiated is 7.37. Thus, as the percentage of relative power increases states initiate a greater number of cyberattacks, and the increase is statistically significant. We now turn to discussing the findings in our descriptive analysis.

Table 1: DV
Number of Initiated Cyber Attacks

Variables	Model 1 DV: Cyber Attack Count
CINC	**7.264** (0.538)***
Polity2	**0.000** (0.003)
Political Rights	**0.012** (0.014)
Civil Liberties	**0.002** (0.014)
Inflation	**-0.000** (0.000)
Trade	**0.000** (0.000)
Battlefield Deaths	**-0.000** (0.000)
Lagged DV	**0.641** (0.026)***
Observations	**944**
r2	**.9497**
Prob. > X2	**.0000****

*p <.10; ** p<.05; ***p<.01; standard errors in parentheses.

Table 2: Predictive Margins
Expected Number of Initiated Cyber Attacks

Independent Variable CINC ScorDV: Cyber Attack Count	**Model 2** DV: Cyber Attack Count
.0	**.0032** (.0092)
.1	**.7296** (.0508)***
.2	**1.4560** (.1042)***
.3	**2.1824** (.1579)***
.4	**2.9088** (.2116)***
.5	**3.6352** (.2653)***
.6	**4.3616** (.3191)***
.7	**5.0881** (.3728)***
.8	**5.8145** (.4266)***
.9	**6.5409** (.4803)***
1	**7.2673** (.5341)***
N	**944**

*p <.10; ** p<.05; ***p<.01; standard errors in parentheses*

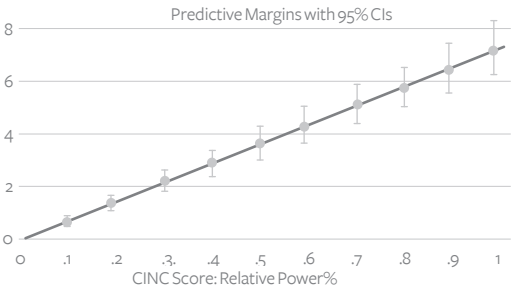

Figure 1: Expected Number of Initiated Cyberattacks

Descriptive Analysis

The descriptive analysis seeks to better understand those factors that affect a state's propensity to cyberattack when considered in the context of the political, economic, and military aspects of the respective attacking and targeted states.[48] This descriptive analysis complements our statistical analysis and includes data on known cyber incidents taken from the CFR COTD from 2005-16 that meet the same criteria used for the statistical analysis. The dataset records

include both cyber attacker and cyberattacked states, and these two categories may not be equal given the multiple players in many of these events. The descriptive analysis includes a total of 102 states.[49] The factors we examine are similar to the factors mentioned in our statistical analysis (State Power and Regime Type) along with State Wealth (Gross Domestic Product: GDP) and two additional conflict measures. We include the two additional measures (Dyadic Conflict and Monadic Conflict) to assess if cyberconflict-involved states are simultaneously involved in traditional forms of military conflicts. We first code whether such Dyadic Conflict refers to states engaged in a crisis/conflict with their cyberconflict counterpart. Monadic Conflict refers to when cyberconflict-involved states are also involved in any other international crises/conflicts. A crisis/conflict includes any event that "leads decision-makers to perceive a threat to basic values, time pressure for response and heightened probability of involvement in military hostilities."[50] The data on military crises/disputes and conflicts were collected from the International Crisis Behavior (ICB) dataset.

Descriptive Results

Several trends emerge when examining the findings from the descriptive analysis. Table 3 of the descriptive results confirms that relative power is a key factor that influences initiation of cyberattacks. The average CINC score for attacking states is .0434, and the average CINC score of targeted states is .0209. Thus, on average, attacking states have twice the amount of relative power than targeted states. In addition, the GDP for attacking states averages 20% higher than that of the targeted state. Attacking states thus generally have greater overall levels of both military and economic power. We conduct a two-sample t-test comparing the mean values of attacking states and targeted states for the relative power measures (CINC and GDP) and in each test the mean values were statistically different at the 99% level.

Table 3: Descriptive Measures

Variables	Mean	Standard Dev.	Minimum	Maximum	Observations
CINC Attacker	.0437295	.0802805	0	.2181166	188
CINC Target	.0209757	.0469934	0	.185799	155
Polity2 Attacker	-2.760638	5.530774	-10	10	188
Polity2 Target	4.877248	4.847779	-10	10	155
Political Rights Attacker	4.710106	2.964542	0	7	188
Political Rights Target	1.909962	1.804903	0	7	155
Civil Liberties Attacker	4.329787	2.736711	0	7	188
Civil Liberties Target	1.901613	1.710458	0	7	155
GDP Attacker	3.86e+12	4.47e+12	0	1.86e+13	188
GDP Target	7.88e+11	1.60e+12	0	9.28e+12	155

Regime type also influences a state's propensity to initiate cyberattacks. Table 3 displays the average Polity2 score of attacking states as -2.7, and 4.8 as the average for targeted states, leaving an average delta of 7.5. The average political rights score for attacking states is 4.71, and 1.9 for targeted states. Similarly, the average civil rights score for attacking states is 4.32 versus 1.90 for targeted states. These findings thus indicate that attacking states have lower overall levels of political rights and civil liberties than targeted states. Further, the Polity2 measure indicates that attacking states are generally more authoritarian than targeted states. Also, we conduct a two-sample t-test comparing the mean values of attacking states and targeted states for the regime type variables (Polity2, Political Rights, and Civil Liberties) and in each test the mean values were statistically different at the 99% level.

Lastly, as to the Dyadic Conflict measure, in 8.17% of cases the attacking state was involved in a crises/conflict with the cyber targeted state(s). In 7.69% of the cases the targeted state was involved in a crisis/conflict with the specific state that it was targeted by in the cyberattack.[51] The Monadic Conflict measure confirmed that the attacking state was involved 16.35% of the time in at least one military crises/conflict with another state when it cyberattacked. Conversely, the targeted state was involved in at least one military crises/conflict with another state in 25.73% of cases when the cyberattack occurred. We conducted a two-sample t-test comparing the mean value of the Monadic Conflict variable for attacking states and targeted states and the results were statistically insignificant. Thus, the difference in mean values for the monadic conflict variable for attacking states and targeted states were not statistically significant.

In summary, in reviewing our descriptive analysis results, relative power, state wealth, and lower levels of democracy appear to increase the propensity to initiate state-sponsored cyberattacks. Cyber aggressors are more likely to have greater levels of power, both militarily and economically, be less democratic, and have weaker political rights and civil liberties. It also appears cyberattacks coincide with military crisis/conflict only in 7%-8% of our cases.

Overall, while regime type (i.e., overall levels of democracy, political rights, and civil liberties) is a factor in a state's propensity to initiate or be targeted by cyberattacks, these political variables are statistically insignificant. Thus, while regime type may be associated with the initiation of cyberattacks (i.e., authoritarian states are more likely to initiate cyberattacks), this effect is not pronounced enough in our sample to have a meaningful effect in our statistical analysis. Rather, state power is the predominant factor that influences cyberaggression in both our statistical analysis and descriptive results. More powerful states are more likely to initiate cyberattacks. These results track findings by scholars that states with greater power initiate more military conflicts than their less powerful counterparts.[52] As with traditional forms of military conflict, power appears to play an important role in influencing state behavior in the cyber realm.

CONCLUSION

This article has considered the relative significance (and insignificance) of a number of factors and their impact on a state's propensity to engage in cyberattacks. We conclude that more powerful and authoritarian states are most likely to initiate cyberattacks. Regime type and state power (both military and economic) are associated with the initiation of cyberattacks. Our statistical analysis also confirms the notion that state power is associated with cyberattack initiation. Here we find that states are more likely to initiate cyberattacks as their relative power increases in the international system. As is true with kinetic military operations, our study confirms that more powerful states are more prone to initiate cyberattacks. Furthermore, in both the statistical analysis and descriptive results, greater power disparity significantly increases the odds of an attack by the stronger on the weaker. These findings further track what we know not only about relative military power but relative economic power as well as it relates to foreign policy behavior.

While this study is a first attempt to examine the factors associated with the initiation of state-sponsored cyberattacks cross-nationally, there is much room for further exploration. For example, which factors influence the severity of cyberattacks, and what is the impact of relative technological sophistication of both attacking and targeted states? Currently, comparative data on the cross-national measures of cyber capabilities of states, is uncharted territory. As this data becomes available, these variables should also be evaluated insofar as how they are influencing cyber conflict. Future research should also analyze what (other than raw power) motivates cyberattacks and why states choose cyberattacks over other alternatives, and how regime type and governance impact this decision, as our descriptive results suggest. This article hopefully has opened the door; more research is now needed to determine precisely how regime type affects cyberconflict.

NOTES

1. P.W. Singer and Allan Friedman, *Cybersecurity and Cyberwar* (New York: Oxford, 2014).
2. Gil Press, "60 Cybersecurity Predictions for 2018" Forbes, November 26, 2017, https://www.forbes.com/sites/gil-press/2017/11/26/60-cybersecurity-predictions-for-2018/#7087bb4073ff.
3. Singer and Friedman, *Cybersecurity and Cyberwar*, 4.
4. Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft," *International Security* 38, no. 2 (2013): 26.
5. Palmer and Morgan, *A Theory of Foreign Policy*.
6. Ragnhild Endresen Siedler, "Hard Power in Cyberspace: CNA as a Political Means," *2016 8th International Conference on Cyber Conflict (Cycon): Cyber Power*, ed., N. Pissanidis, H. Rõigas, and M. Veenendaal, 23-36, (Tallinn: NATO CCDCOE Publications, 2016), 26.
7. Siedler, "*Hard Power in Cyberspace.*"
8. Ibid.
9. Ibid.
10. Jon R. Lindsay and Lucas Kello, "Correspondence: A Cyber Disagreement," *International Security* 39, no. 2 (2014): 29.
11. Daniel Hughes and Andrew M. Colarik, "Predicting the Proliferation of Cyber Weapons into Small States," *Joint Force Quarterly* 83, no. 4, 21.
12. Siedler, "*Hard Power in Cyberspace.*"
13. Adam P. Liff, "Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War." *Journal of Strategic Studies* 35, no. 3 (2012): 401-428.
14. Brian M. Mazanec, *The Evolution of Cyber War: International Norms for Emerging-Weapons Technology* (Lincoln, NE: Potomac Books, 2015).
15. Siedler 2016; Fred Kaplan, *Dark Territory - The Secret History of Cyber War* (New York: Simon & Schuster, 2016).
16. Thomas Rid, *Cyber War Will Not Take Place* (New York: Oxford University Press, 2016).
17. P.W. Singer and Emerson T. Brooking, *LikeWar: The Weaponization of Social Media.* (New York: Houghton Mifflin Harcourt, 2018).
18. Erik Gartzke and Jon R. Lindsay, "Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace," *Security Studies* 24 (2015): 335.
19. David C. Gompert and Phillip C. Saunders, *The Paradox of Power: Sino-American Strategic Restraint in an Age of Vulnerability* (Washington, D.C.: National Defense University Press, 2011).
20. Bruce M. Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World* (Princeton: Princeton University Press, 1993).
21. Bruce Bueno de Mesquita and Randolph Siverson, "War and the Survival of Political Leaders: A Comparative Study of Regime Types and Political Accountability," *American Political Science Review* 89, no. 4 (1995).
22. Steve Chan, "Mirror, Mirror on the Wall ...Are the Freer Countries More Pacific?" *Journal of Conflict Resolution* 28, no. 4 (1984).
23. Dan Reiter and Erik Tillman, "Public, Legislative, and Executive Constraints on the Democratic Initiation of Conflict," *Journal of Politics* 64 no. 3 (2002).
24. Darren Filson and Suzanne Werner, "Bargaining and Fighting: The Impact of Regime Type of War Onset, Duration and Outcomes," *American Journal of Political Science* 48, no. 2 (2004).
25. Rebecca MacKinnon, "Liberation Technology: China's 'Networked Authoritarianism'," *Journal of Democracy* 22, no. 2 (2011).
26. MacKinnon, "Liberation Technology: China's 'Networked Authoritarianism'," 33.
27. Ibid., 44.
28. Ron Deibert and Rafale Rohozinski. (2010), "Control and Subversion in Russian Cyberspace.," In Ronald Deibert, John Palfrey, Rafel Rohozinksi, Jonathan Zittrain, and Miklos Haraszti (eds), Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace (Cambridge: MIT Press), 15-34.
29. Ron Deibert and Rafale Rohozinski, "Liberation vs. Control: The Future of Cyberspace," *Journal of Democracy*, 21, no. 4 (2010): 50.

NOTES

30. Ron Deibert, "Authoritarianism Goes Global: Cyberspace Under Siege," *Journal of Democracy*, 26, no. 3 (2015): 65.
31. Deibert, "*Authoritarianism Goes Global,*" 65.
32. Ibid., 68.
33. Ibid., 68.
34. Jan Kallberg, "Strategic Cyberwar Theory-A Foundation for Designing Decisive Strategic Cyber Operations," *The Cyber Defense Review* 1, no. 1 (2016): 114.
35. Kallberg, "*Strategic Cyberwar Theory*", 114.
36. Ibid., 116.
37. Council on Foreign Relations, "Cyber Operations Tracker Dataset" (2018), https://www.cfr.org/interactive/cyber-operations, May 11, 2019.
38. See the (CFR 2018) Dataset for more information regarding the data collection methodology.
39. David J. Singer, Stuart Bremer, and John Stuckey (1972), "Capability Distribution, Uncertainty, and Major Power War, 1820-1965;" In Bruce Russett (ed) Peace, War, and Numbers, Beverly Hills: Sage, 19-48.
40. Halvard Buhaug. "Dude, Where's My Conflict? LSG, Relative Strength, and the Location of Civil War," *Conflict Management and Peace Science* 27, no. 2 (2010):107-128.
41. J. David Singer, Stuart Bremer, and John Stuckey, "Capability Distribution, Uncertainty, and Major Power War, 1820-1965;" In *Peace, War, and Numbers*, ed. Bruce Russett (Beverly Hills: Sage, 1972).
42. Polity IV Project, *Polity IV data set* (College Park, MD: University of Maryland, Center for International Development and Conflict Management, 2014).
43. Todd L. Allee and Paul K. Huth, "Legitimatizing Dispute Settlement: International Legal Rulings as Domestic Political Cover," *American Political Science Review* 100, no. 2 (2006).
44. Freedom House (2014) "About Freedom in the World: An annual study of political rights and civil liberties."
45. The trade variable measures trade as a percentage of annual GDP for each state. The inflation variable captures the percentage of inflation for each state for each year.
46. World Development Indicators (WDI 2014).
47. For more on hypothesis testing please see David F. Groebner, Patrick W Shannon, and Phillip C. Fry, "Business Statistics," 9th Edition, Chapter 7 (London: Pearson, 2013).
48. The variation in the years included in the statistical analysis and descriptive analysis is due to the variation in the years covered (i.e., data availability) for the variables required for the statistical analysis.
49. Only states involved in cyber incidents are included in the descriptive analysis.
50. Michael Brecher and Jonathan Wilkenfeld, A Study of Crisis (Ann Arbor, MI: University of Michigan Press, 2000); Michael Brecher et al., International Crisis Behavior Data Codebook, Version 12 (2017, 4).
51. Percentages vary for the dyadic conflict measure for attacking and targeted states due to the unequal number of attacking versus targeted states in the sample.
52. Palmer and Morgan, *A Theory of Foreign Policy*.