The Victims of Cyberspace:

Factors that Increase Cyber Harm Severity

Allison Moore

IR-6690 XTIA- Capstone Course

September 23, 2022

Abstract

With the proliferation of technology, states have evolved their ability to exert power in cyberspace, unleashing a range of cyber harms upon victim states. There is little research in current literature which explores the factors that impact how cyber harms manifest and propagate throughout states. Uncovering the factors that lead to more sever cyber harms may assist policy makers in making decisions in regard to cyberspace. Through the use of ordinal logistic regression, an inverse relationship is discovered between democracy and cyber harm severity. Furthermore, there is adequate evidence indicating that the presence of data protection and privacy laws leads to less severe cyber harms. Ultimately, this research is a modest contribution to the literature on cyber harms, providing a small platform for future researchers to expand the discussion on cyber harm victims and cyber harm severity.

Introduction

In 1988, the first computer worm was released by Cornell graduate student Robert Morris (Federal Bureau of Investigation 2018). Although the program did not destroy any files, Morris's Worm still devasted numerous university and military electronic functions, with several entities resolving to remove computers from their networks or wiping the computers completely. The Federal Bureau of Investigation (2018) reports that the damages resulting from Morris's Worm began at $100,000 and reached into the millions.

With the proliferation of technology since 1988, states have taken a note from Robert Morris and evolved their ability to exert power in cyberspace, unleashing a range of *cyber harms* upon victim states. Agrafiotis, et al. (2016, 2) define *cyber harms* as the "damaging consequences resulting from cyber-events." Cyber-events and their resulting cyber harms can be either intentional or unintentional and can originate from states, non-state actors, and/or individuals. Regardless of the intent of the sender, victim states can experience a variety of types and severity of cyber harms.

In this paper, I will focus on cyber victim states. I intend to explore the relationship between regime type, digital landscape, and severity of cyber harms. I will begin with an evaluation of current literature on cyber harms. Next, I will explain the methodology before presenting the research results. The results will be followed by an in-depth discussion on the findings and a conclusion summarizing the major findings and considering what they may mean for future studies.

Cyber Harms Throughout the Literature

Current literature on cyber harms falls into two very distinct frames of reference: first, the Cybersecurity perspective which tends to focus on the technical aspects of cyber tools and their impacts; second, the International Relations (IR) point of view which shifts attention to how actors interact with each other and exert power in cyberspace. The overwhelming majority of literature is framed from the perspective of the sending state, with a few outliers who expand upon the cyber harms experienced by the victim states. Until recently, most research focused on theory rather than developing and testing hypotheses. Kello (2013, 9-15) attributes this theoretical focus to the "paradoxical" problem of having both too little and too much data to test hypotheses with any degree of certainty. However, the available data has changed substantially over the last decade.

Those researchers and works that fall into the category of focusing on the sending state tend to concentrate on cyberweapons, offensive and legal policy, escalation, deterrence and signaling.

Theorists such as Kello (2013, 8) note that "cyberweapons are not overtly violent," which distinguishes them from the traditional kinetic forms of war. Many researchers agree with his assessment and, as a result, have propagated the belief that a "Cyber Pearl Harbor" (i.e., cyber harms consisting of substantial loss of life and/or significant physical destruction) is not possible. Gartzke (2013,58-9) also subscribes to this idea, noting that cyber harms are temporary and can only have long term effects if

the sending state pairs cyber capabilities with kinetic ones. Furthering the idea of pairing cyber operations with conventional military capabilities, Buchanan (2020) highlights to versatility and flexibility of cyber capabilities in geopolitics. He ultimately concludes that cyber operations are flawed tools of deterrence and signaling because attribution and intention are incredibly difficult to determine in cyberspace (Buchanan 2020).

Outside of physical harms and deterrence, the concept of cyberweapons also led to the question of how to apply these offensive cyber capabilities (OCOs) to inflict desired cyber harms. Smeets (2018) breaks OCOs into two distinct categories: counterforce cyber capabilities (CFCC) and countervalue cyber capabilities (CVCC). He concludes that CFCCs tend to target military infrastructure and cause less direct damage than CVCC, while CVCCs tend to target critical infrastructure (Smeets 2018, 94). Although these categories are useful for classifying sending state OCOs, they do not effectively elaborate on the relationship between targeting and resultant cyber harms.

Through most similar qualitative analysis, Kemmer broadens the idea of incorporating cyber capabilities into state policies by uncovering the answer to how sending states can utilize cyber capabilities for coercion. Kemmer (2021) ultimately finds that sending states can utilize cyber capabilities for coercive measures; because many governments will absorb the financial costs of cyber harms enacted against private industries and organizations, cyber harms can lead victim states to adapt their behavior. Understanding the offensive capabilities available to states is certainly important when considering sending state policies and procedures; however, OCO tools

do not currently provide enough insight into understanding how cyber harms impact and permeate throughout the victim state.

Several researchers also venture into the realm of cyber governance and the applicability of current international law to cyberspace. Following Russia's cyber-attack against Estonia in 2007, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) (2022) developed the Tallinn Manual, which analyzes how international law applies to cyberspace, but is not legally binding. Lotrionte (2021, 100) also summarizes the implications of the UN Charter framework on state cyber activity and ultimately concludes that the cyber 'gray zone' will reduce over time as international law evolves and states tend towards more structured cyber norms. She brings light to an incredibly important concept: the *effects-based approach.* Lotrionte (2021, 81-2) highlights the fact that considering the effects of an attack- rather than the intent of the attack- is essential for determining legal ramifications for state actions. This concept is incredibly important when assessing the type and severity of cyber harms and will serve as the foundation for this paper.

More recent literature in this category has shifted from qualitative study to quantitative analysis. In one of the very first works to shift the discussion to how regime type impacts international cyber relations, Hedgecock (2021, 41) provides substantial empirical evidence indicating that there is no statistically significant difference between democracies and autocracies on the likelihood of initiating cyber operations in a given year; she finds that autocracies initiate cyber operations at a greater frequency in a given year than democracies and that democracies are more likely to target the private sector than autocracies. This work marks a shift in cyber harm literature from dyadic

analysis to large-n monadic analysis but leaves the reader wondering how regime type can impact the other half of the dyad.

Only a few writers weigh cyber harms from the perspective of the victim state. Current cyber harm literature considering victim state points of view focus on categorizing, rather than analyzing, cyber harms.

Linking the Cybersecurity and IR disciplines, Agrafiotis, et al. (2016, 33-5) define and map the “layers of cyber harm,” which include how simultaneous harms, cascading effects, and latent harms populate across individuals, organizations, and nations. They conclude their research by listing possible metrics for evaluating cyber harms, but ultimately note that there are not reliable measurements available for all types of cyber harm (Agrafiotis, et al. 2016, 37). Agrafiotis, et al. (2018) also leveraged their findings from 2016 to develop a taxonomy of cyber harms, where they created five primary categories which were validated through case study analysis: physical or digital harm, economic harm, psychological harm, reputational harm, and social/ societal harm. These five categories are further broken down into numerous subsets which can aid in assessing the harms that result from cyber operations. It is important to note that the cyber harm taxonomy was designed considering cyber effects within an organization, rather than a state. Although this taxonomy offers the most descriptive categorization for cyber harms within the literature, there are currently no indices available to effectively assess these harms (e.g., the only current international reputation index is limited to 28 countries (Fernandez-Crehuet, et al. 2021)).

Lastly, Valeriano and Maness (2014, 359) apply theories on regionalism and rivalry as they develop the Dyadic Cyber Incident and Campaign Dataset (DCID) and conclude that cyber disputes result in minimal effects and are rare. While their work takes a dyadic approach, Valeriano and Maness do attempt to expand upon the victim state experience through the addition of cyber harm variables in their dataset. The DCID 2.0 includes a ten-point scale for the severity of a cyber incident and four categories for cyber "damage types" which include combinations of Direct, Indirect, Immediate, and Delayed effects (Maness, Valeriano, et al. 2022). These damage types roughly correspond to the layers of cyber harm developed by Agrafiotis, et al.

Although cyber harms are frequently discussed in the literature, most works focus primarily on the attacking state, the OCO capabilities they possess, and the policy options available to influence the behavior of a victim state. There is an obvious lack of research on victim states and the factors that lead to increased levels of cyber harm. This leads to a few unanswered questions. Is there a significant difference in how cyber harms manifest and propagate in a democracy versus an autocracy? If so, what factors contribute to this difference?

Research Design

With the ubiquity of internet enabled technology comes the opportunity for more frequent and severe cyber harms. Gartzke and Lindsay (2015, 316) attribute increased volumes of cyber-attacks to “societal dependence on the Internet” and note that cyber aggressors utilize the same channels as “legitimate commerce and communication.” Gartzke and Lindsay’s theory implies a direct correlation between the frequency of cyber incidents and the extent of a state’s digital integration. Considering that 8 of the top 10 states for Digital Competitiveness are democratic (of these, 6 are fully democratic with a PolityV of +10), there is likely more opportunity for cyber harm within a democracy than an autocracy (International Institute for Management Development 2021). This theory leads to the following hypotheses which will be tested in this paper:

H1. Democratic states are more likely to experience more severe cyber harms than autocracies.

H2. States with the least developed digital landscapes experience the least severe cyber harms.

H2a. States with privacy and protection legislation experience less severe cyber harms.

In this research, I will use ordinal logistic regression to explore the causal relationship between regime type, state digital landscape, and the severity of cyber harms. The unit of analysis is an individual victim state for a given cyber incident. All data used will range from 2005 to 2018- due data limitations- and will be recorded for the calendar year specified in the DCID 2.0 interaction end date (Maness, et al. 2022).

The end date of a cyber incident will be used rather than the start date based on two assumptions: because many cyber harms are not noticed and/or analyzed until after the cyber incident has ended; and because some cyber incidents do not end until the victim state has been alerted to the incident due to the presence of cyber harms. As discussed earlier in the paper, this research relies upon the logic of Lotrionte's effects-based approach. In total, there are 333 cases available for analysis.

The Variables

The dependent variable in this study is the severity of cyber harms (SEV) as defined by Maness, et al. (2022) in their DCID 2.0 database. This categorical variable ranges from 0 to 10, where 0 represents no cyber damage and 10 represents massive loss of life (i.e., more than 100 lives lost).

The first independent variable is the regime type of the victim state, as measured by Marshall and Gurr's PolityV (PVV) (2020). This variable ranges from -10 (full autocracy) to +10 (full democracy).

This study also includes five additional independent variables that consider the digital landscape of the victim state. These variables account for Gartzke and Lindsay's theory that more technological capabilities allow more opportunity for cyber aggression. The first variable is the share of Information, Communication, and Technology goods as a percentage of total state trade (ICT) (UNCTADSTAT 2022). ICT provides insight into the victim state economic dependence upon technological goods. The next independent variable representing the victim state technological landscape is the number of

individuals using the internet (INT), represented as a percent of the total population of the victim state (World Bank 2022). Next is the Networked Readiness Index (NRI) rank (World Economic Forum 2022). The NRI ranking will be used, rather than the NRI value, to mitigate the effects of adjustments made to the NRI coding over the last 20 years. For any years missing NRI rankings, the previous year's NRI ranking will be used. Any states that are not included in the NRI will be recorded as the last rank for the given year. Although the ICT and INT variables are two of the 60 variables included in the modern NRI, not all years account for the variables in the same manner, so each has been included on their own. Lastly, the presence of Data Protection and Privacy Laws (DPPL) and Consumer Protection Laws (CPL) are included as binary independent variables where 1 represents the presence of the law for the given year (UNCTAD 2022). The content of the laws is not considered.

To control for the possible deterring nature of the victim state hard power, the Global Firepower (2022) ranking (GFP) will be used. To compensate for changes to GFP coding over time, the ranking is used rather than the GFP value. Those victim states who did not rank in the top 25 for the specified year have been coded as "33."

The method used to conduct the cyber operation (METH) will also be a control variable as some methods are more likely to result in less severe cyber harms than others. METH is a DCID 2.0 categorical variable with the following value assignments: 1-Vandalism, 2-Denial of Service, 3-Network Intrusion, 4- Network Infiltration, 4.1- Logic Bomb, 4.2- Virus, 4.3- Worm, and 4.4-Key Logger (Maness, et al. 2022). Additionally, the study will control for the type of target through the variable TYPE because some targets are naturally more susceptible to increased levels of cyber harm than others.

TYPE originates from the DCID 2.0 categorical variable Critical Infrastructure which ranges from 1 to 17 and represents the type of infrastructure attacked within the victim state (Maness, et al. 2022).

The Method and the Models

Because the dependent variable is an ordered categorical variable (0 to 10, increasing in severity), ordinal logistic regression will be used. Prior to implementing the regression, the numerical independent and control variables will be normalized using min-max normalization. This normalization will mitigate any possible issues arising from the presence of negative variables; however, it will also impact how we interpret the resultant coefficients for the variables. Ordinal logistic regression essentially provides odds ratios for the selected variables which indicate how the probability of SEV's value changes with changes in the selected variables. Each value of SEV will have its own resultant equation with a unique intercept value; however, the coefficients for the independent and control variables will remain constant across the values of SEV. Due to the choice to normalize the data, each e^(coefficient) will represent the odds ratio of the maximum value of a variable, as compared to the minimum value of a variable.

Four separate models will be tested. Model 1 serves as a baseline for regime type and includes PVV and the control variable GFP. The second model consists of the five digital landscape variables and the control variable GFP. This will provide a baseline indication of the digital landscape's impact on SEV. Model 3 essentially combines Model 1 and Model 2 with the five digital landscape variables, PVV, and GFP

to provide an indication of how a victim state's digital integration and polity impact the severity of the cyber harms it experiences. Lastly, Model 4 includes all independent and control variables. Model 4 will provide a holistic view of how regime type and digital landscape affect cyber harm severity, considering the attack methods used and the target type. Because METH and TYPE are expected to have a significant impact on SEV, these control variables are only assessed in Model 4. This will allow for adequate consideration of the relationships between the independent variables and SEV.

Results and Discussion

Table 1 displays the resultant coefficients and standard errors for each of the four models following ordinal logistic regression. The control variable, GFP, demonstrates no significance throughout the models. However, there are some indications that there is likely some deterring effect caused by a strong kinetic force in a victim state. Because GFP is represented as a ranking, lower values correspond to increased firepower capabilities. One of the first indicators of the deterring effect of GFP is that the coefficients are positive in most of the models (i.e., high ranking states experience less severe cyber harms). There is also a negative correlation between GFP and PVV. This indicates that democracies tend to have a higher GFP ranking than autocracies. The implications of this relationship are discussed below through the analysis of PVV across the models.

Table 1

Ordinal Logistic Regression Results

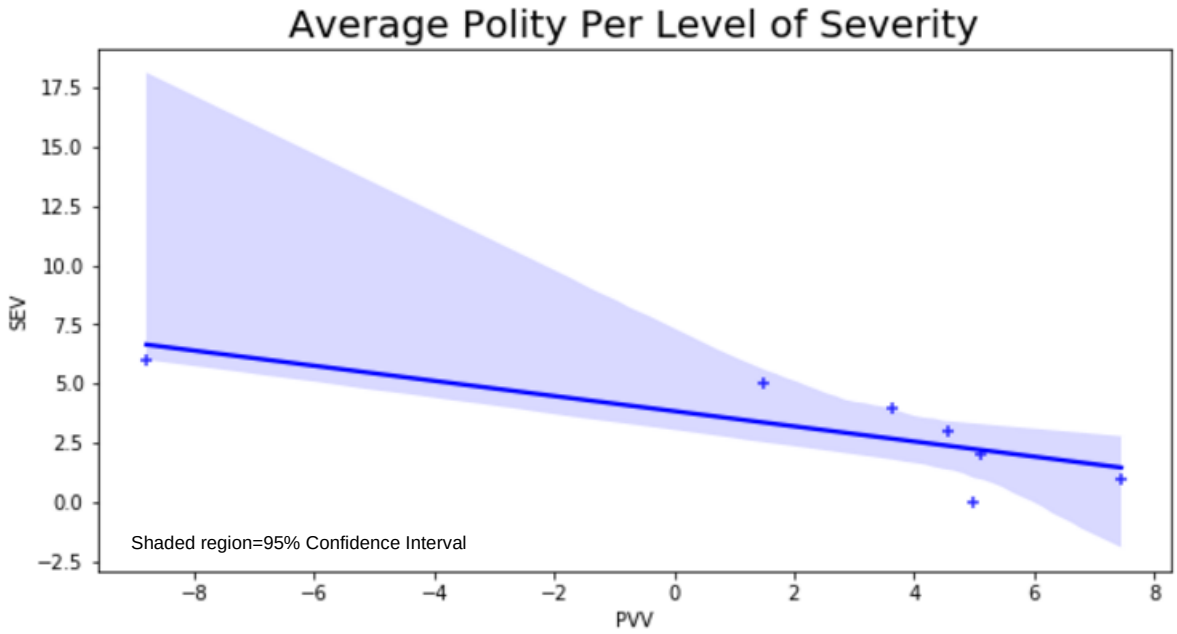
	Model 1	***Model 2***	***Model 3***	***Model 4***
	Coefficient (Std error)	*Coefficient (Std error)*	*Coefficient (Std error)*	*Coefficient (Std error)*
PVV	-0.936 (0.330)**		-1.752 (0.565)**	-0.987 (0.580)
GFP	-0.172 (0.309)	0.406 (0.376)	0.170 (0.387)	0.279 (0.388)
NRI		0.326 (0.533)	-1.305 (0.748)	-1.124 (0.746)
ICT		-0.063 (0.433)	-0.398 (0.447)	-0.816 (0.460)
INT		1.937 (0.503)	0.965 (0.591)	0.166 (0.611)
DPPL		-0.057 (0.366)	0.011 (0.368)	-0.27 (0.374)
CPL		-0.273 (0.315)	-0.034 (0.326)	-0.034 (0.333)
TYPE				-0.557 (0.487)
METH				4.898 (0.532)***

***P ≤.01* ****P ≤.001*

The evidence shows a significant inverse relationship between regime type and the severity of cyber harms experienced as a result of a cyber incident in Model 1 and Model 3. Although the confidence interval drops for PVV in Model 4, regime type retains a similar negative coefficient. This negative correlation is further displayed by the average polity score of each category of severity, as shown in figure 1. The 95% confidence interval in figure 1 assists in visualizing the concept that the odds of a full autocracy (-10) experiencing more severe cyber harms than a full democracy (+10) are 1/(e^-.936) ~ 2.5 times the odds of the reverse. These odds are increased to 5.7 with the addition of the digital landscape variables in Model 3. The inverse relationship between PVV and SEV throughout all models directly invalidates hypothesis 1 and demonstrates that autocracies are more likely to experience more severe cyber harms than democracies.

Figure 1

Averaged Polity Across Each Severity Category

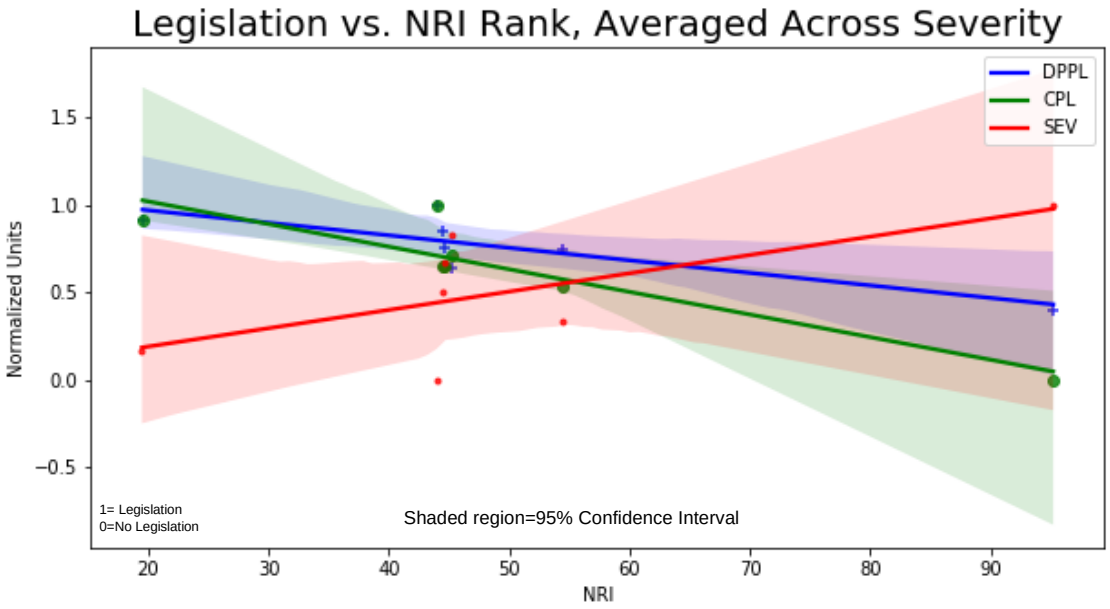


Although none of the digital landscape variables demonstrate significance across the models, there is relative continuity in the direction of many of the coefficient signs. Due to the use of rank for NRI, a negative coefficient indicates that more network ready states experience less severe cyber harms (i.e., higher ranking states experience less severe harms). However, analysis through averaging the NRI rank for each level of severity offers a volatile relationship at larger severities and lower NRI ranks, validating the insignificance presenting in table 1. Although the inverse relationship presented at low severity levels is not in line with Gartzke and Lindsay's theory, the additional digital landscape variables can help to provide some rationale for the discrepancy at higher NRI ranks.

As table 1 indicates, the presence of data protection and consumer protection laws share an inverse relationship with the severity of cyber harms. Figure 2 displays this correlation by depicting the average DPPL and CPL at each severity category versus NRI rank. In the figure, DPPL, CPL, and SEV are plotted using normalized values for purposes of scaled comparison. Hence, all plotted y-values fall between 0 and 1. As a reminder, DPPL and CPL are binary variables where 0 indicates the lack of legislation, and 1 represents the presence of legislation. The figure indicates that states who adopt DPPL and CPL legislation experience less severe cyber harms (i.e., there is an inverse relationship between presence of legislation and the level of cyber harm severity), which can provide some insight into why the NRI variable presents in the opposite direction. States with more advanced network infrastructure and capabilities (higher NRI rank) tend to institute digital protection laws, possibly muting the effects of cyber harms.

Figure 2

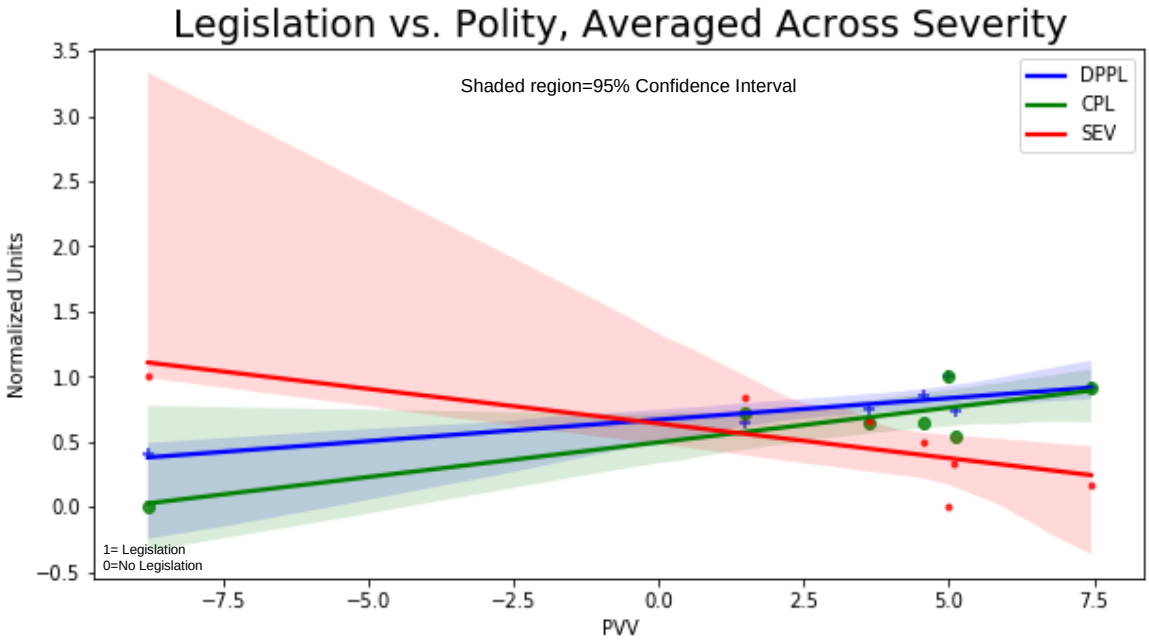
Average Legislation Presence Versus Average NRI Rank with Severity Level



Furthermore, figure 3 demonstrates the positive correlation between PVV and the presence of legislation. Similar to figure 2, figure 3 uses a normalized y-axis for comparison of multiple variables. The relationships shown in figure 3 further indicate that democracies, which are the primary states with high NRI rankings, are more likely to institute DPPL and CPL legislation. In fact, NRI and PVV demonstrate a strong inverse correlation (-0.77) (see Appendix for all variable Pearson correlation values) which supports the concept that democracies tend to have higher NRI rankings. It is also interesting to note that the presence of DPPL offers greater odds of less severe cyber harms than the presence of CPL (DPPL odds ratio= 1.3, CPL odds ratio=1.0). This may be caused by the frequency of cyber incidents which target data acquisition versus cyber incidents which target consumer goods industries and consumers directly; however, this warrants further investigation.

Figure 3

Average Legislation Presence Versus Average Polity with Severity Level



The INT and ICT variables present insignificant results with no notable insight provided through the consideration of how these variables average across the categories of severity. This may be attributed to the targeted nature of the cyber incidents provided in the data which target critical infrastructure categories. Of the 333 cases used, 143 cases target the Government Facilities Sector (see the Appendix for more statistics on the data). This likely skews the data towards cyber harms which are less reliant upon victim state domestic populaces for the propagation of the harms and could contribute to the insignificant nature of INT and ICT.

Altogether, the digital landscape variables do not adequately test hypothesis 2. Considering the insignificance of the relationship between the digital landscape variables and SEV, as well as the volatility surrounding NRI, hypothesis 2 is inconclusive. There simply isn't enough confidence or consistency in the relationships to

satisfactorily identify an answer for hypothesis 2. However, for hypothesis 2a, there is suitable evidence supporting the idea that states with privacy and protection laws experience less severe cyber harms than states who do not have these types of legislation. There is also substantial correlation between hypothesis 1 and hypothesis 2a; that is, democratic states have a higher incidence of adopting privacy and protection laws and are less likely to experience increased severity of cyber harms.

With the implementation of additional control variables in Model 4, METH stands out as the most significant variable in the analysis of cyber harm severity. The strong, positive relationship between METH and SEV is expected and easily explained. Worms and viruses are innately more damaging than simple cases of vandalism because they are able to replicate and propagate across the internet and are often destructive in nature. The incorporation of the method used to impart cyber harms is an insufficient substitute for the attacker's intent, which is often impossible to determine. Even though METH retains the greatest significance in the study and is the only significant variable in Model 4, PVV maintains its negative coefficient in Model 4 at a value similar to that found in Model 1. This allows for a fair amount of confidence in testing hypothesis 1. As noted above, the TYPE variable is greatly skewed towards the Government Facilities Sector. Although this may have a negative impact when considering INT and ICT, the most-similar nature of the cyber incidents actually solidifies the relationship between PVV and SEV as it minimizes the effects that a more diverse set of targets could impart. But this leaves the study with less external validity than is usually attributed to quantitative analysis.

All four models performed at low levels of accuracy. Models 1-3 performed around 38% accuracy, while Model 4 performed at 56% accuracy. The substantial jump in accuracy in Model 4 speaks volumes about the importance of the target type and method utilized to impart cyber harms in determining the resultant severity of the cyber harms. The low levels of performance across the board also imply that there are other important variables missing from this study which impact the severity of cyber harms within a victim state. Many of these missing variables may be linked to the categories of cyber harms specified by Agrafiotis, et al. For example, stemming from Agrafiotis, et al.'s (2018) psychological cyber harms, a state's cultural considerations may impact how psychological harms manifest and propagate throughout the domestic populace, ultimately affecting the severity of the cyber harms. Consideration of these types of variables lie outside the scope of this research but offer future authors a platform for more advanced inquiries into cyber harm severity.

Conclusion

Three hypotheses derived from Gartzke and Lindsay's theory on increased cyber incidents with societal dependence on the internet were tested using four models of ordinal logistic regression. There is strong evidence that democracies are less likely to experience higher levels of cyber harm severity than autocracies. Furthermore, the data also show that states who employ consumer and data protection laws are less likely to experience higher levels of cyber harm severity than states who do not enact these types of laws. These two relationships are likely connected because there is evidence

suggesting that, on average, democracies are more likely to enact protective data and consumer laws.

Other concepts arose throughout the research that require further review in future research. More thorough analysis of why data protection laws offer greater odds of less severe cyber harms than consumer protection laws is needed. Although this study retains the external validity associated with quantitative analysis, it also maintains internal validity due to the targeted nature of the data. Another study on this topic should broaden the data used to targets outside of critical infrastructure. To achieve this, researchers will have to adapt a monadic database, such as the Council on Foreign Relations (2022) Cyber Operations Tracker, to the coding used in the DCID 2.0. Building this type of database will likely take a significant amount of time and is open to subjectivity in the interpretation of the DCID 2.0 coding. Additionally, more research is needed to understand how a state's digital landscape contributes to the effects of cyber incidents. Future study on this may require the development of numerous indices and the application of Agrafiotis, et al.'s (2018) comprehensive cyber harm taxonomy to evaluate the second and third order impacts of cyber operations in a victim state.

Ultimately, the findings in this paper are a modest contribution to the literature on cyber harms. The relationships between cyber harm severity, polity, and the presence of data protection laws have minor policy implications as they lie either in the realm of common sense (logic concludes that data protection laws minimize damage), or outside of the realm of practicality (shifting state polity towards full democracy to increase the odds of less severe cyber harms is no easy feat). However, the study provides another avenue for uncovering the factors that make states more resilient to cyber harms which

may encourage future in-depth investigations. It is also important to consider the fact that the correlations presented in this study do not equate to causation. Future studies can help to uncover the true causalities behind these relationships through qualitative analysis.

Bibliography

Agrafiotis, Ioannis, Maria Bada, Paul Cornish, Sadie Creese, Michael Goldsmith, Eva Ignatuschtschenko, Taylor Roberts, and David Upton. 2016. “Cyber Harm: Concepts, Taxonomy and Measurement.” *University of Oxford.* Saïd Business School RP 2016-23. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828646. (Accessed August 2, 2022).

Agrafiotis, Ioannis, Jason R. C. Nurse, Michael Goldsmith, Sadie Creese, and David Upton. 2018. “A Taxonomy of Cyber-Harms: Defining the Impacts of Cyber-Attacks and Understanding How they Propagate.” *Journal of Cybersecurity*. 4(1):1-15. DOI: 10.1093/cybsec/tyy006. https://academic.oup.com/cybersecurity/article/4/1/tyy006/5133288?searchresult=1. (Accessed August 1, 2022).

Buchanan, Ben. 2020. *The Hacker and the State: Cyber Attacks and the New Normal of Geopolitics.* Cambridge: Harvard University Press.

Council on Foreign Relations. 2022. “Cyber Operations Tracker.” https://www.cfr.org/cyber-operations/. (Accessed August 25, 2022).

Federal Bureau of Investigation. 2018. “The Morris Worm: 30 Years Since the First Major Attack on the Internet.” https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218

Fernandez-Crehuet, J.M., J. Rosales-Salas, and S. Diaz Cogollos. 2021. “Country’s International Reputation Index.” *Corporate Reputation Review* 24: 14-30. https://doi.org/10.1057/s41299-019-00088-8.

Gartzke, Erik and Jon R. Lindsay. 2015. “Weaving Tangled Webs: Offense, Defense, and Deception in Cyberspace.” *Security Studies.* 24(2): 316-348. DOI: 10.1080/09636412.2015.1038188.

Global Firepower. 2022. “GlobalFirepower.com Ranks: Military Powers Ranked Since 2005 According to Global Firepower.” https://www.globalfirepower.com/global-ranks-previous.php. (Accessed September 2, 2022).

Hedgecock, Kathryn J. 2021. “Deciphering the Implications of State-Sponsored Cyber Operations for IR Theory.” Stanford University. http://purl.stanford.edu/yj410vw9056. (Accessed August 4, 2022).

International Institute for Management Development. 2021. “World Digital Competitiveness Ranking.” https://www.imd.org/centers/world-competitiveness-center/rankings/world-digital-competitiveness/. (Accessed September 12, 2022).

Kello, Lucas. 2013. “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft.” *International Security.*38(2): 7-40. http://www.jstor.com/stable/24480929.

Kemmer, Tara A. 2021. “Hacking for Peace: The Case for Cyber Coercion.” Boston University Graduate School of Arts and Sciences. https://open.bu.edu/handle/2144/43020. (Accessed August 5, 2022)

Lotriionte, Catherine. 2018. “Reconsidering the Consequences for State-Sponsored Hostile Cyber Operations Under International Law.” *The Cyber Defense Review*. 3(2): 73-114. https://www.jstor.org/stable/10.2307/26491225.

Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Benjamin M. Jensen, and Jose M. Macias. 2022. *The Dyadic Cyber Incident and Campaign Dataset, version 2.0,* available at: https://drryanmaness.wixsite.com/cyberconflcit/cyber-conflict-dataset.

Marshall, Monty, G. and Ted Robert Gurr. 2020. “Polity5 Project, Political Regime Characteristics and Transitions, 1800-2018.” *Center for Systemic Peace.* https://www.systemicpeace.org/inscrdata.html. (Accessed August 14, 2022).

NATO Cooperative Cyber Defence Centre of Excellence. 2022. “About Us.” https://ccdcoe.org/about-us/. (Accessed August 21, 2022).

Smeets, Max. 2018. “The Strategic Promise of Offensive Cyber Operations.” *Strategic Studies Quarterly*. *12*(3): 90–113. http://www.jstor.org/stable/26481911.

United Nations Conference on Trade and Development. 2022. “Summary of Adoption of E-Commerce Legislation Worldwide.” https://unctad.org/topic/ecommerce-and-digital-economy/ecommerce-law-reform/summary-adoption-e-commerce-legislation-worldwide. (Accessed 2 September 2022).

United Nations Conference on Trade and Development STAT. 2022. “Share of ICT Goods as Percentage of Total Trade, Annual.” https://unctadstat.unctad.org/wds/TableViewer/tableView.aspx?ReportId=195158. (Accessed 2 September 2022).

Valeriano, Brandon and Ryan C. Maness. 2014. “The Dynamics of Cyber Conflict Between Rival Antagonists, 2001-11.” *Journal of Peace Research.* 51(3): 347-360. http://www.jstor.org/stable/24557484.

World Bank. 2022.” Individuals Using the Internet (% of Population).” https://data.worldbank.org/indicator/IT.NET.USER.ZS. (Accessed August 24, 2022).

World Economic Forum. 2022. “Network Readiness Index.” *Portulans Institute.* https://networkreadinessindex.org/. (Accessed September 8, 2022).

Appendix

All data, tables, and figures can be found at https://github.com/almo214/MSIRCapstone. The Jupyter Notebook file (.ipynb) contains basic descriptive information, a correlation heatmap, outliers plot, data skewness figures, value counts for categorical variables and additional figures not used in the research report.