Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study

Ahmet Selçuk Arslan

Department of Political Science and International Relations, Marmara University, Istanbul, Turkey

Ahmet Selçuk Arslan is a senior student of Political Science and International Relations B. A. programme at Marmara University.

a.selcuk616@hotmail.com

ORCID iD: 0000-0001-8635-3402

1. Abstract

Two crucial factors have urged IR scholars to account for state behaviour in cyberspace: the increasing volume of cyber attacks and the rising scale of damage induced by these attacks. These have led to a series of initiatives appealing to the grand theories of IR in order to scrutinize state behaviour in depth, particularly regarding the securitization and militarization of cyberspace. Following a similar pattern, this work intends to contribute to IR literature by presenting a neorealist analysis of state behaviour in cyberspace by relying on quantitative methods. Two regression analyses, one using a linear algorithm and the other using a negative binomial algorithm, were conducted using a dataset consisting of 4,099 samples. The analyses indicate that as states build more cyber security capacity, they tend to engage in more disruptive actions against other states in cyberspace. Both regression models were subsequently trained using artificial neural networks (ANNs) for robustness check, which enhanced the results computed by the traditional models.

2. Keywords

realism; neorealism; security dilemma; cyberpolitics; cyber security

3. Introduction

Cyberspace has been characterized as the fifth domain of warfare almost for one and half decade, beside air, space, sea and land (Azmi et al., 2016). Two crucial factors have urged IR academia to account for state behaviour in cyberspace; one is the increasing volume of cyber attacks in recent years (USDOE, 2022), and

https://doi.org/10.33774/apsa-2023-www2z-v8 **ORCID:** https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. **License:** CC BY 4.0

the other is the raising scale of damage induced by these attacks[1] (Dunn Cavelty and Wenger, 2020). These developments have made states more sensitive and demanding on the issues pertaining cyber security, leading them to establish their own peculiar national cyber security strategies (NCSS) (Luiijf et al., 2013). Although not universally agreed upon, there is a widely accepted idea that building defensive mechanisms in the age of information technology and of internet is much harder and more expensive than adopting offensive initiatives (Drezner, 2019; Lynn III, 2010; Mohee, 2022; Nakashima, 2015; O'Hanlon, 2018). This makes executing detrimental actions, such as cyber attacks, in the cyberspace more appealing both for states and non-state actors.

Motivated by an incentive to bring an explanation to this offense-defence balance, this work strives for bringing a theoretical framework to cyber politics by applying the concept of "security dilemma" on states' endeavour in pursuit of the militarization and the securitization of cyberspace. By doing so, I intend to give an answer from a neorealist perspective to the question that "does states' cyber security capacity building increase their tendency to execute detrimental actions against other states in cyberspace?". I hence took states' cyber security capacity as the independent variable, and states' dissemination of false information in foreign countries and the number of state-sponsored or executed cyber attacks as the dependent variables. The study relies purely on quantitative methods—particularly on linear and negative binomial regression analyses—to justify its hypotheses. Two datasets were taken from different data repositories and were merged into a single dataset, which included 4,099 samples in total. Subsequently, the dependent variables were analysed on multivariate basis. Two follow-up ANN models were created to execute robustness testing.

4. Previous relevant work

A retrospective look unfolds that, back into the first decade of the 21st century, several attempts were made to scrutinize and explain the relationship between state security and cyberspace to which the work of Bendrath (2001) was an example, arguing that sustaining a stable and effective cyber security policy would be challenging for states particularly under liberal order where infrastructure providers are mostly from private companies. Nonetheless, this and such works either remained shallow in terms of providing a theoretical framework on security, or their remarking remained nothing more than assumptions due to the lack of adequate scientific data of the time and of relevant case studies that demonstrate the outcomes of cyber (in-)security and of cyber warfare. A parenthesis should be put here to state that the very existence of the term "cyber war" or "cyber warfare" has always been controversial. I would prefer to dichotomize these types of works falling into the debate on whether the conflicts in cyberspace can evolve into a scale of "warfare"; "the camp of deniers" and "the camp of endorsers". One of the most prominent works in the camp of deniers belongs to Rid (2013). His and alike works' fundamental arguments commonly revolve around the idea that actions taken in cyber space may have real-world implications, however, their results cannot be devastating

[1] See, for instance, Baezner M and Robin P (2017) Hotspot Analysis: Stuxnet. Center for Security Studies (CSS), ETH Zürich, Zürich.

than conventional acts of violence. He furtherly underlines that competition and rivalry between states given in cyber domains can be resolved before evolving into a great scale real-world war. I would therefore prefer to locate his work within the liberal theoretical tradition. On the other hand, it is a commonly accepted idea both in the camp of deniers and the camp of endorsers that one of the most, or maybe the most, conspicuous feature(s) of cyber venues is its facilitatory role in the acts of espionage, DoS (denial of service), propaganda, identity theft, sabotage, and so forth (Choucri, 2012b; Denning, 2001; Greathouse, 2014; Inkster, 2010; Kassab, 2014; Kremer and Müller, 2014; Luiijf, 2012; Steed, 2011). I therefore point out that the primary takeaway from such works is that there is little to no debate about whether cyber world enables such malicious actions; the main point of controversy is *to what extent* states bear to go for extraordinary offensive measures against one another as a consequence of these actions.

Such attempts were followed by the emergence of highly suspicious notions on the applicability of theory on cyber venues in terms of security issues, drawing attention to the gap of theoretical framework and on the incompatibilities of the current traditional IR theories to explain security-related state attitude in cyber realm (Eriksson and Giacomello, 2006). Going on a deeper level, Eriksson and Giacomello (2006) argued that non-state actors possess less power in the cyber realm compared to states, however, they are gradually gaining strength. Certain novel works, on the contrary, underlined the shifting balance of power in cyber space streaming towards non-state actors, which have commenced to hold, in some cases, more power even than states (Schmitt and Watts, 2016). Therefore, I argue that a liberal perspective may be proposed to explain the very peculiar characteristics of cyber domains by drawing attention particularly on the power of non-state actors. What counts as "power" in the cyber realm is a blurry issue, though; if it is counted as capacity to influence, Kremer and Müller 2014 define it as "the direction of (public) opinion by either providing, shaping or withholding information". They continue and underline the empowering impacts of ICT (Information Communication Technologies) in terms of non-state actors by quoting the words of Dartnell (2003): "(ICT provides) enormous opportunities for non-state actors and enhances the global profile of previously marginalised issues and movements".

A great number of works published in the last decade have challenged the validity of such notions. It is noteworthy to mention of the work of Tumkevič (2019) falling to this branch in the sense that her perspective is relatively similar to the one used in this study. In her work, she specifically draws attention on the emergence of a "negative cooperation" between US-China and US-Russia in cyberspace by subscribing to the perspective of defensive realism. Watanabe (2020), on the other hand, particularly deals with "capacity building" in cyberspace and provides a more general framework by applying three major IR theories (Liberalism, Realism, and Constructivism), thus, explaining military capacity building in cyberspace with realism, economic capacity building with liberalism, and normative capacity building with constructivism. Again, even though his work provides the literature with a qualified point of view from the lenses of the grand theories of IR, the validity of these finding remains questionable without relying on a grounded data. In his analysis on Stuxnet cyber attack incident in 2010 (Baezner and Robin, 2017), Mohee (2022) concludes that anarchical nature of cyberspace makes offensive incentives more tempting, and cyber capabilities of states contribute to their survival. This is still a matter of great debate among scholars and is commonly accounted by referring to the offense-defence theory of Robert Jervis (Glaser and Kaufmann, 1998; Jervis, 1978; Quester, 2002; Slayton, 2017). Although a consensus yet to be reached, most of scholarly works point out that developments in cyber technologies favour offensive actions. As indicated by Shaheen (2014), utilization of cyber weapons mostly for offensive actions but not for defensive purposes would tilt the offense-defence balance in favour of aggression, resulting in the destabilization of the international security system. Even though this study does not position offense-defence theory at its centre as the chief theory of explanation, it implicitly relates the adoption of defensive measures with offensive action and how increasing capacity for the former may subsequently contribute to the execution of the latter, triggering a vicious spiral.

Moreover, Pytlak and Mitchell (2018) went one more step further and conducted a quantitative study on the incentives that trigger a cyber activity between states, discovering that nuclear power status of a state may be a driving force of cyber conflict. There lies a similar motive behind the logic of this study. As seen in the aforementioned studies above, majority of the works that seek bringing a theoretical perspective on cyber security-related issues lack a quantitative data analysis to reinforce their findings. This gap also limits the improvement of existing theories, and the development of new theoretical perspectives. This work therefore intends to put forth a satisfactory realist point of view anchored in a quantitative analysis conducted by using historical data.

5. Realist Understanding of Cyber Security, Its Implications, and Security Dilemma

There exist two concepts which had and have been appreciated by realist thinkers above everything else; power and security, both of which tightly complement each other. The concept of “security” is commonly attributed to four basic elements; physical safety, autonomy, development, and rule. There can be no compromise on the notion established by the realist consensus that both physical safety and autonomy are indispensable components of security. Nevertheless, certain realists may assign relatively less significance to the aspects of 'autonomy' and 'development'. This attitude subjected to criticisms by some prominent realist thinkers in the sense that overlooking the developmental aspect may result in bitter consequences for a nation, as it implicitly contributes to the relative national power (Morgan, 2007). Increasing awareness of states about how cyber attacks may result in devastating outcomes that explicitly undermine national security appreciated the attributed importance on and precedence of cyber security, vaulting its cruciality to the national security level (Dewar, 2018). Cyber security, hence, is not considered a matter of low politics but high politics (Dunn Cavelty, 2008). Therefore, I find fair to say the fact that emergence of cyber challenges cements the undeniability of the developmental aspect of security in the realist school of thought.

One foremost and identical characteristic of cyberspace that it shares with the realist assumption of a real-world political system is its anarchical structure (Adams, 2001; Choucri, 2012c; Kiggins, 2014; Nye Jr, 2022), lack of an upper authority above states. Whilst classical realist thought considers domestic elements and the human nature as the chief driving forces of state behaviour, neorealist school of thought emphasizes the impact of the way how international system is structured in shaping state behaviour (Joseph, 2014). Moreover, challenging the classical realist assumption that links international conflicts to human nature and state-level factors, neorealists attribute the emergence of conflicts primarily to the anarchical nature of the system. These distinct ideas also reflect on the methodological techniques appreciated by the classical realists and neorealists; classical realists favouring a more human-centring and historical approach, and neorealists favouring a systematic analysis that particularly focus on understanding the impact of the distribution of power among states. These assumptions make neorealism a suitable theory to scrutinize state behaviour in cyber space in the sense that cyber space, similar to the real-world international system, is an anarchic medium where there is no upper authority to check and control the conflicts in it. In addition, the appropriateness of cyberspace for systematic analysis stems from its inherent potential, which can be evaluated using relevant techniques, including the measurement of states' cyber power.

More on the anarchy, the structural realist theory of Waltz (1979) takes the anarchy as the chief point of departure that urges states to seek power to ensure their security. Power is therefore not seen as an end but only as a "tool" to reach the very ultimate goal; survival. By the same token, the state is just a virtual being seen in cyberspace among other actors, such as hackers, other cyber terrorist groups, and sometimes NGOs, against whom its chief purpose is maintaining its security and existence in the realm. One may therefore postulate that in a medium where non-state actors hold considerable amount of power that contribute to the configuration of cyber landscape, states have no choice but to focus on ensuring their own "survival" in the realm by leveraging the means known as "cyber security", which is achievable through security maximization. Indeed, this does necessarily not mean that states are free of offensive initiatives in cyberspace. I just want to underline that non-state actors may have the upper-hand over states in terms of offensive actions thanks to four characteristics of cyberspace that specifically favour non-state actors; *permeation* (penetrates boundaries and jurisdictions), *participation* (reduces barriers to activism and political expression), *attribution* (obscures identities of actors and links to action), and *accountability* (bypasses mechanisms of responsibility)[2].

This postulation brings forth the question that how—or if—security dilemma manifest in cyberspace in the light of the security understanding of states in cyberspace mentioned above? Security dilemma emerges as a consequence of the possibility of the dual-use of capacity (Herz, 1951; Jervis, 1978). This means that technological innovations made by a state to improve its level of development in cyber technologies also increase its capacity to utilize these technologies in a disruptive manner, threatening internal and/or external security of victim(s). I therefore argue that increase in the cyber security capacity of states amplifies their tendency to utilize cyber power in a disruptive manner.

[2] See Table 1.1 in; Choucri N (2012a) New Challenges to International Relations Theory and Policy. In: Cyberpolitics in International Relations. Cambridge, MA 02142: The MIT Press, p. 4 .

$\boldsymbol{H_0}$ = *Raise in the cyber security capacity of states has no particular effect over the tendency of the utilization of cyber power in a disruptive manner.*

$\boldsymbol{H_\alpha}$ = *Raise in the cyber security capacity of states increases the tendency of the utilization of cyber power in a disruptive manner.*

6. Research Design

The study takes “cyber security capacity” as the independent variable (IV), and “utilization of cyber power in a disruptive manner” as the dependent variable (DV). The existing literature provides academia with vast amounts of datasets to measure a given country’s security in cyberspace in numerical values. Nonetheless, for data providers, surveying explicit state aggression or state-sponsored cyber attacks is much more challenging than assessing cyber infrastructure protection. This issue makes it complicated for this study to examine available data that are suitable to be adapted on the dependent variable. I therefore preferred to rely on two different but interrelated dependent variables. One is the number of cyber operations executed by states, and the other is the dissemination of false information on virtual platforms against foreign states.

I intend to make further clarifications on the latter dependent variable; what is covered within the context of “dissemination of false information abroad”? It covers the actions undertaken by the state in question on social media, blogs, forums, the internet channels of news moguls, or in any other internet medium to diffuse synthetic information, or disinformation. The chief objectives of doing so range from promoting, justifying, and appreciating disinformation that favours the disseminating government to falsifying, trivializing, and sometimes antagonizing distributors of genuine information that disfavours the disseminating party. It is a common practice to execute these initiatives both through, for instance, real and bot accounts on Twitter and Facebook. All these actions are considered to be part of information warfare given on the internet—take the role of Russia in the US presidential elections in 2016 as an example[3] (The Guardian, 2017).

My research design relies on two different regression algorithms. The data for the independent variable were sourced from the 'government cyber security capacity' index of Varieties of Democracy Project (V-Dem) version 13 (V-Dem Coders, 2023). According to the coders of this data, the scores for all countries have been transformed from ordinal to interval using a measurement model. I collected the scores for each individual country in the dataset from 2000 to 2022, as no data were available before 2000. The dataset contains an ample sample size (4,099 in total), providing a robust foundation for conducting a consistent and meaningful analysis. Similarly, the data concerning the first dependent variable (government dissemination of false information abroad) originate from the V-Dem project. The data regarding the second dependent variable (cyber operations by country) were acquired from a separate source, the Council on Foreign Relations (CFR) (2023). Their dataset records each known state-sponsored cyber attack between 2005 and 2022. I collapsed

[3] For further clarifications and examples, see Tai H (2022) Russia’s dissemination of false information. Available at: https://v-dem.net/weekly_graph/russias-dissemination-of-false-information.

https://doi.org/10.33774/apsa-2023-www2z-v8 ORCID: https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. License: CC BY 4.0

these data into numerical values, reflecting the instances of cyber attacks carried out by each country in specific years. Subsequently, I compiled two datasets: one containing V-Dem data and the other consisting of Council on Foreign Relations (CFR) data. I consequently merged these two datasets into a single dataset using a 'join' method. In the first model, where the dissemination of false information is the dependent variable, no missing values were identified in any variables, including controls and the dependent variable itself. For the second model, I initially constructed a negative binomial regression model to predict missing values in the second dependent variable (number of cyber attacks). Subsequently, I replaced all missing values with the predictions generated by this initial model. Finally, I created a genuine negative binomial regression model using the dataset where missing values in the second dependent variable had been replaced with these predictions.

The process of cybersecurity capacity building does not solely rely on technical flourishment (Clark et al., 2014a); managerial, social, legal, policy, and regulatory aspects of development are also considered the very components of this process (Clark et al., 2014b; Creese et al., 2021; Dutton et al., 2019; GCSCC, 2021). In this context, it is hence feasible to incorporate defamation protection into the study as a confounding variable. This is because defamation protection illustrates the extent to which cyber law is robust and effectively enforced in a country, thereby offering insights on the advancement of that country's cybersecurity capacity. On the other hand, government internet filtering capacity and government capacity to regulate online content are the indicators that simply demonstrate the technical capabilities of states to remain their supremacy in cyber space intact against domestic rival figures (GCSCC and CICTE, 2020; The White House, 2011, 2023). These rationales thereby make these three variables suitable for use as control variables in the analyses.

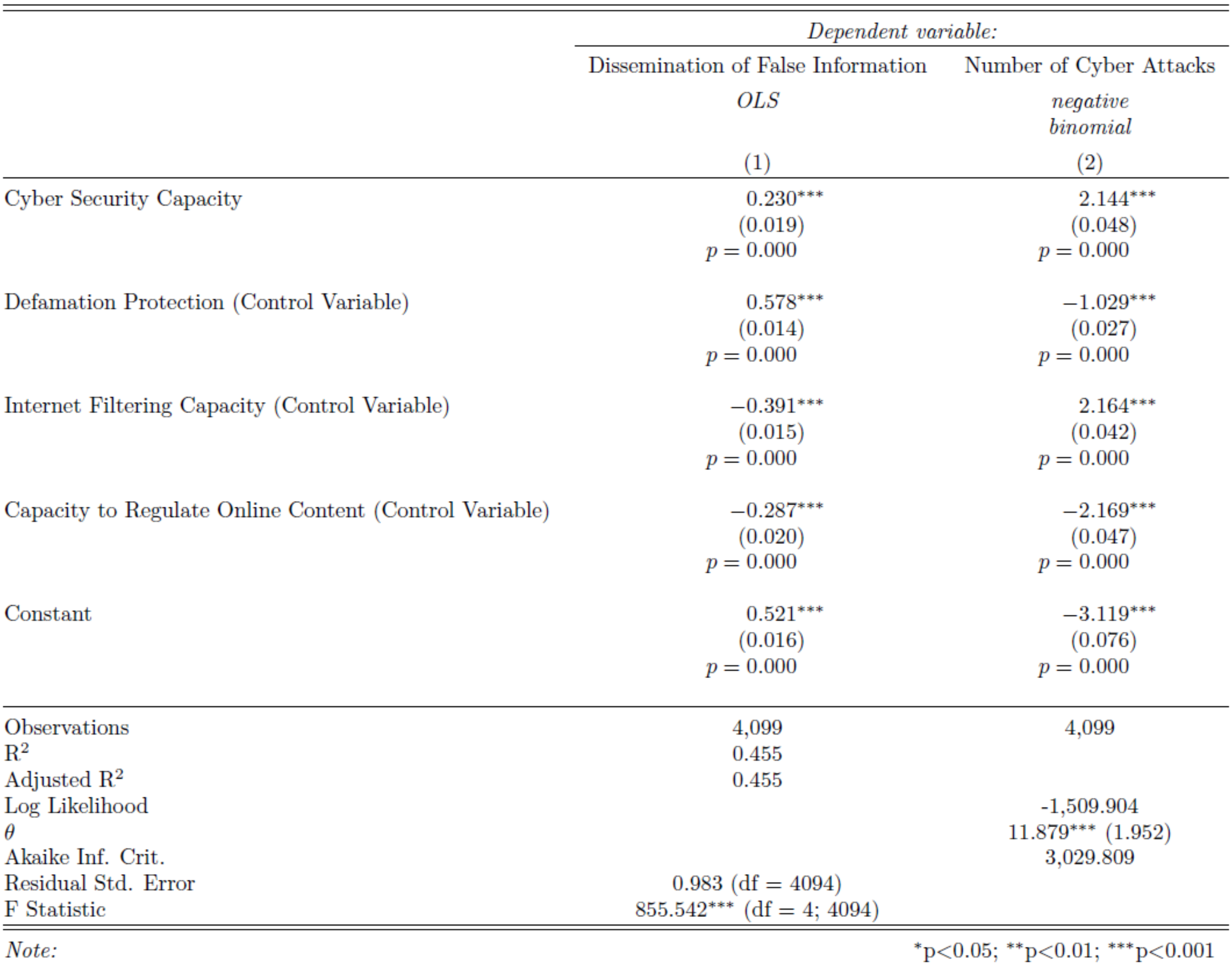
Measurements applied on the independent and the dependent variables are likewise applied on the control variables. One regression model is produced for each DV, first of which is a linear model (OLS), as the first DV is a continuous data scaled to interval. The second model is built of negative binomial regression algorithm since the second DV is a count data where the variance (5.503028) is greater than the mean (0.6028). I used R language to carry out all these operations and to create a regression coefficient plot. Python language is subsequently used for building two artificial neural network (ANN) models to execute robustness check.

7. Results

Table 1 and **Figure 1** indicate the numerical results of the analyses.

https://doi.org/10.33774/apsa-2023-www2z-v8 **ORCID:** https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. **License:** CC BY 4.0

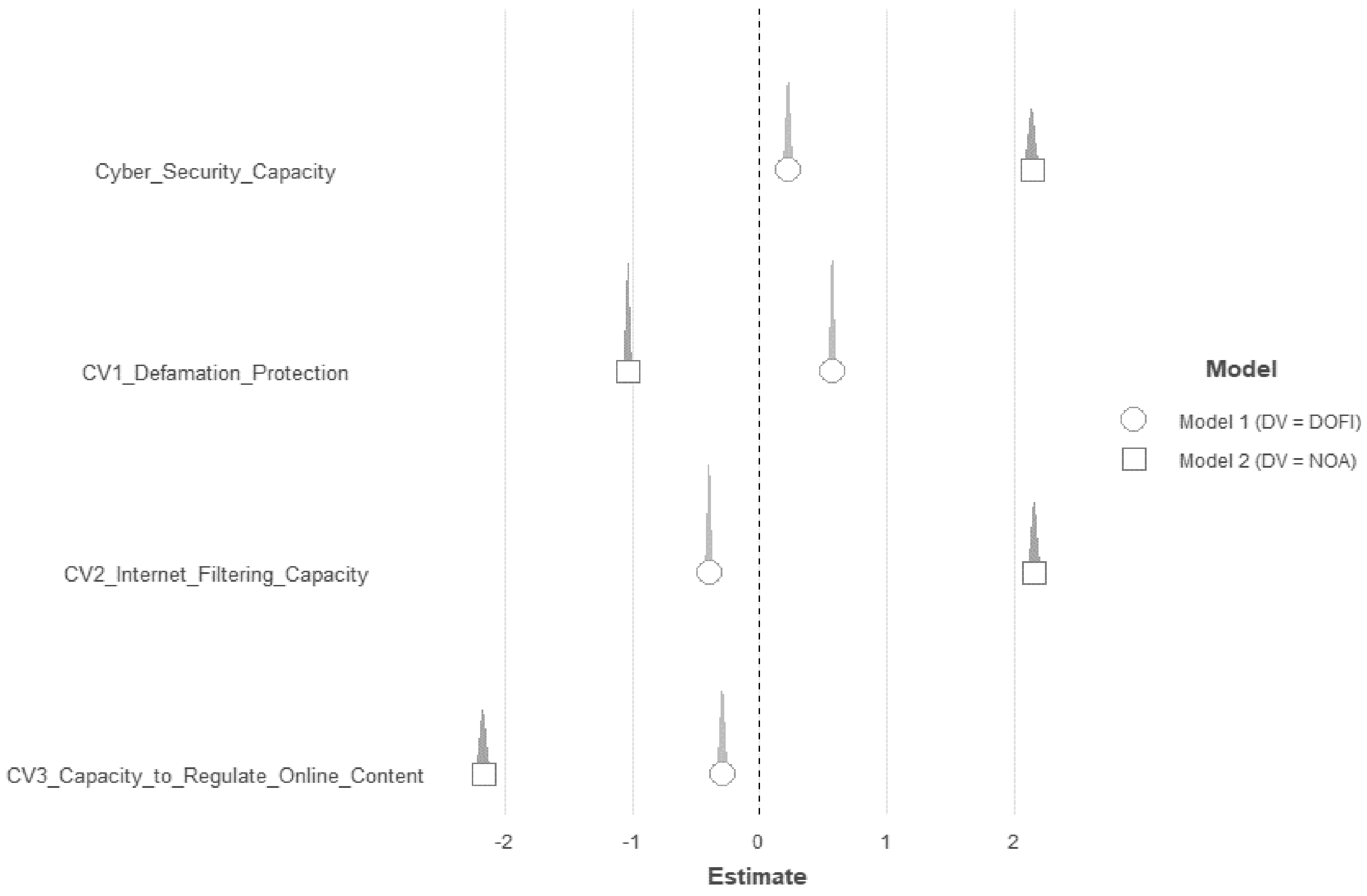
Table 1: Multivariate regression results



	Dependent variable:	
	Dissemination of False Information	Number of Cyber Attacks
	OLS	*negative binomial*
	(1)	(2)
Cyber Security Capacity	0.230*** (0.019) $p = 0.000$	2.144*** (0.048) $p = 0.000$
Defamation Protection (Control Variable)	0.578*** (0.014) $p = 0.000$	−1.029*** (0.027) $p = 0.000$
Internet Filtering Capacity (Control Variable)	−0.391*** (0.015) $p = 0.000$	2.164*** (0.042) $p = 0.000$
Capacity to Regulate Online Content (Control Variable)	−0.287*** (0.020) $p = 0.000$	−2.169*** (0.047) $p = 0.000$
Constant	0.521*** (0.016) $p = 0.000$	−3.119*** (0.076) $p = 0.000$
Observations	4,099	4,099
R^2	0.455	
Adjusted R^2	0.455	
Log Likelihood		-1,509.904
θ		11.879*** (1.952)
Akaike Inf. Crit.		3,029.809
Residual Std. Error	0.983 (df = 4094)	
F Statistic	855.542*** (df = 4; 4094)	
Note:		*p<0.05; **p<0.01; ***p<0.001

All variables (including controls) in both models yielded highly statistically important results by falling below $P < 0.01$ threshold and not containing the value zero ("0") within respective confidence intervals, as shown in **Figure 1**. On the other hand, whilst cyber security capacity and defamation protection are found to have a positive-sided relationship with the DV in the first model, internet filtering capacity and capacity to regulate online content are found to have a negative association. In spite of its positive linear relationship with the DV in the first model, it is found by the second model that defamation protection is associated with a negative linear relationship with the number of cyber attacks. Reversely, internet filtering capacity indicated a negative association with the first DV but a positive association with the second DV. These results indicate that an increase in cyber security capacity is associated with both an increase in the dissemination of false information abroad and the number of state-executed or sponsored cyber attacks. The null hypothesis ($\boldsymbol{H_0}$) is successfully rejected in favour of the alternative hypothesis ($\boldsymbol{H_\alpha}$); executing disruptive actions in cyberspace becomes a more common practice for a country when its cyber security capacity raises.

Figure 1: Regression coefficient plot



Several iterations are conducted on the model 1 to find out the most optimal density values. It is eventually found that the ANN architecture of the model 1 with the most ideal validation loss comprised of two hidden layers with twelve neurons on both layers. **Figure 2** and **Figure 3** visually demonstrate the architecture of the model.

Figure 2: ANN architecture of the Model1 in FCNN style

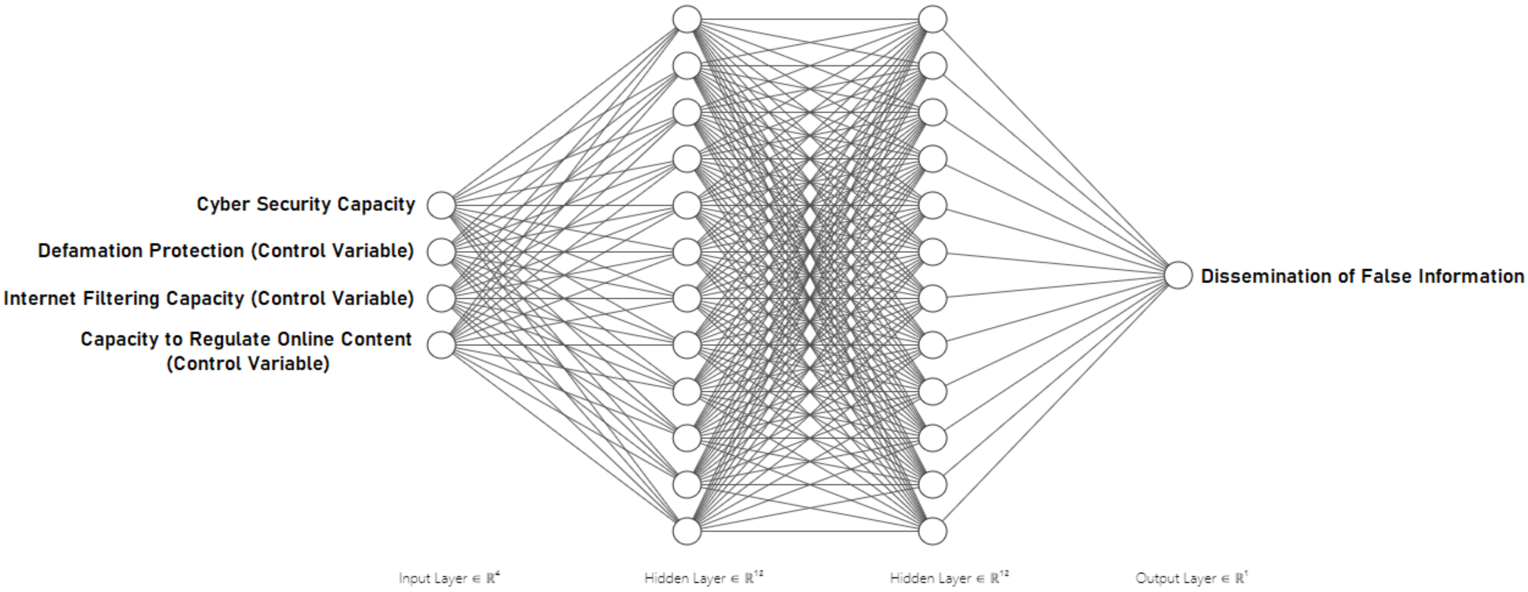
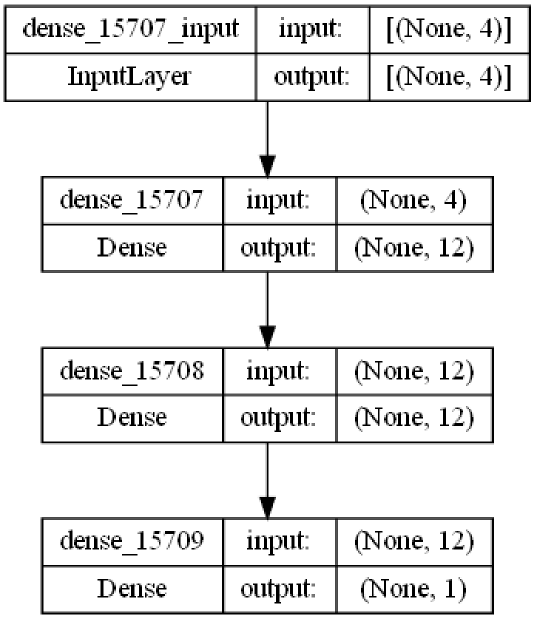

Cyber Security Capacity
Defamation Protection (Control Variable)
Internet Filtering Capacity (Control Variable)
Capacity to Regulate Online Content (Control Variable)
Dissemination of False Information
Input Layer ∈ ℝ⁴
Hidden Layer ∈ ℝ¹²
Hidden Layer ∈ ℝ¹²
Output Layer ∈ ℝ¹

Figure 3: Keras plot of the Model1



dense_15707_input	input:	[(None, 4)]
InputLayer	output:	[(None, 4)]

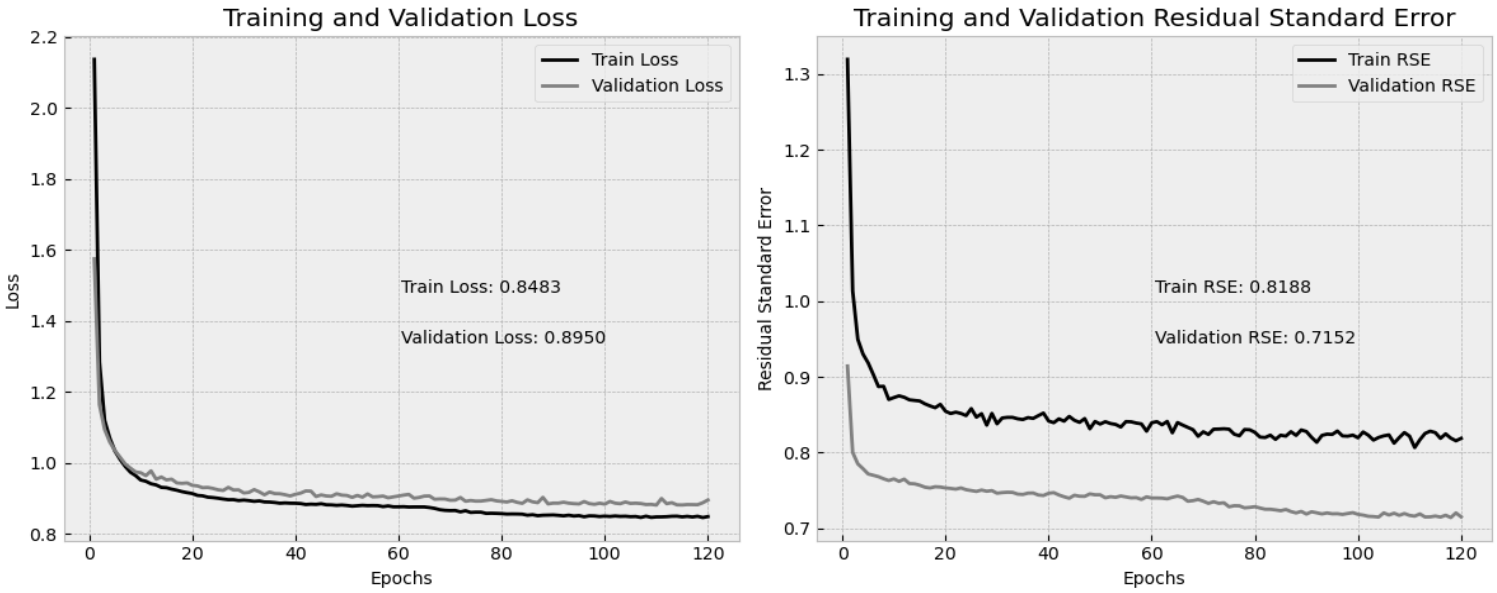
dense_15707	input:	(None, 4)
Dense	output:	(None, 12)

dense_15708	input:	(None, 12)
Dense	output:	(None, 12)

dense_15709	input:	(None, 12)
Dense	output:	(None, 1)

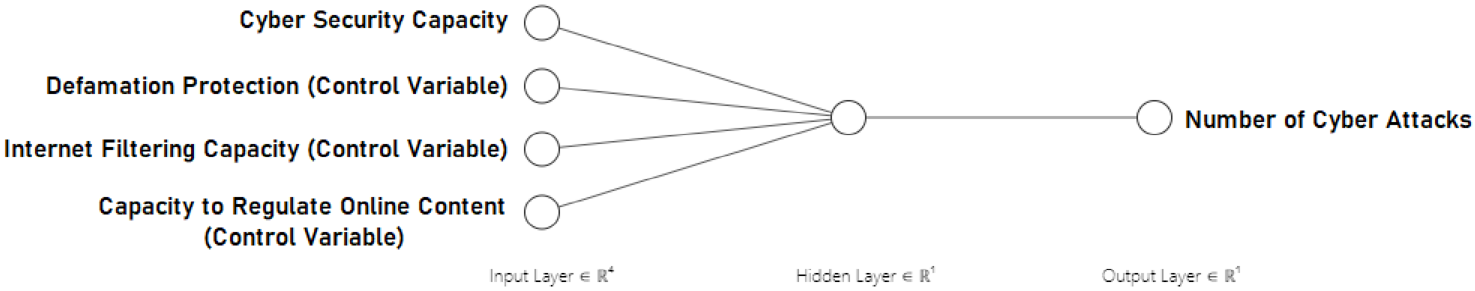
Methods that are applied on the Model1 to prevent the over-fitting were L2 regularization, k-fold cross-validation, and early stopping. Three different lambda values are iterated over the model (0.001, 0.01, 0.1). The most ideal lambda value for L2 regularization turned out to be 0.01 hereby. The data were divided into ten folds using k-fold cross-validation, with a maximum number of epochs limited to two hundred and a batch size of eight. Lastly, early stopping with the patience value of ten is applied and the training sequence is thereby stopped when the performance of the model started to degrade. Residual standard error (RSE) of the model is traced in order to compare the efficiency of the ANN model with the traditional OLS model. "Rectified linear unit" (ReLU) is used as the activation function in the hidden layers, and "Linear" function is used in the output layer. **Figure 4** demonstrates the training process along with the final RSE and loss values. An improvement with 0.2678 less RSE is seen in the ANN model vis-à-vis the traditional model $(0.9830 - 0.7152)$. Neither over-fitting nor under-fitting were observed in the ANN model.

Figure 4: Training sequence of the Model1



I applied same procedures to create the most optimal architecture for the model 2. However, the second model failed to yield an accurate ANN model without overfitting the model. I therefore removed L2 regularization for the model 2. As shown in the **Figure 5** and **Figure 6**, the most optimal ANN architecture of the model 2 is computed to have a single hidden layer with one neuron. "ReLU", which is applied on the hidden layer, and "Exponential", which is applied on the output layer, activations were used for this model.

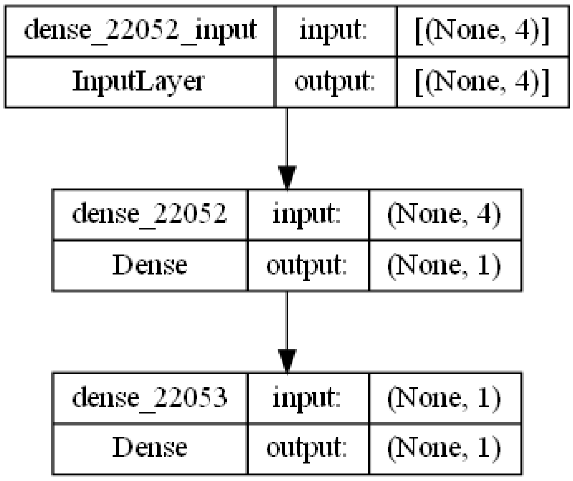
Figure 5: ANN architecture of the Model2 in FCNN style



Cyber Security Capacity
Defamation Protection (Control Variable)
Internet Filtering Capacity (Control Variable)
Capacity to Regulate Online Content (Control Variable)
Number of Cyber Attacks
Input Layer ∈ ℝ⁴
Hidden Layer ∈ ℝ¹
Output Layer ∈ ℝ¹

https://doi.org/10.33774/apsa-2023-www2z-v8 **ORCID:** https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. **License:** CC BY 4.0

Figure 6: Keras plot of the Model2



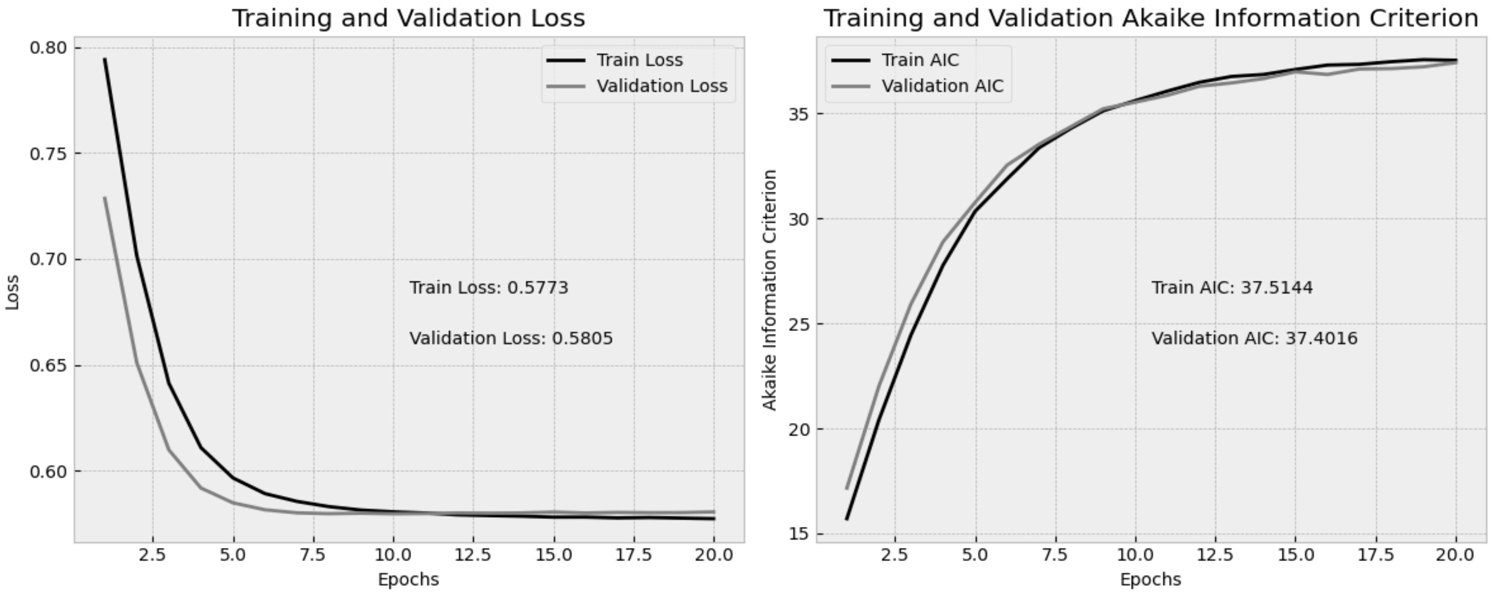
dense_22052_input	input:	[(None, 4)]
InputLayer	output:	[(None, 4)]

dense_22052	input:	(None, 4)
Dense	output:	(None, 1)

dense_22053	input:	(None, 1)
Dense	output:	(None, 1)

Akaike Information Criterion (AIC) was used as the goodness-of-fit metric for comparing the performance of the ANN model with the traditional negative binomial regression model. A substantial improvement was observed in the ANN model with a decrease of 2992.4 in AIC value $(3029.8 - 37.4)$. Neither over-fitting nor under-fitting were observed in the ANN model. **Figure 7** shows the training sequence of the Model2.

Figure 7: Training sequence of the Model2



8. Discussion and Conclusion

By their nature, ANN models tend to be more complex than traditional models, resulting in more challenging interpretation of their produced results. Nevertheless, they are also more effective in revealing intricate relationships between variables. I trained both of my ANN models by utilizing cross-validation techniques to ensure their robustness and generalizability. Moreover, the performance metrics computed by the ANN models exhibited considerable improvements when contrasted with the metrics derived from the traditional models. Hence, these facts collectively reinforce the credibility and reliability of the outcomes obtained through the traditional OLS and negative binomial regression models, enhancing the trustworthiness of the study's conclusions.

Security dilemma is one of the key tenets in the realist understanding of international politics. As it has widely been referred by the scholars in the realist school of thought in order to ascribe explanations on state behaviour and foreign policy in the real world, it is also possible for us to apply this concept on state actions in the cyberspace as well. The results I got by this quantitative analysis urge me to underline one point; as I mentioned in the previous sections, chief driver of state attitude in the cyberspace is ensuring its security as any vulnerability may be exploited by non-state aggressors to undermine its tangible assets, such as infrastructure (The White House, 2000). However, the results furtherly indicate that states also do not hesitate to use the capacity they built for security purposes to breach other states' security, which means that security challenges of states in the cyberspace is not given solely to non-state actors, but also to other states. This finding therefore makes this study more suitable to be put on the offensive line of neorealism, indicating that states commonly tend to see cyber capacity building no different that "cyber power building" which might be used against other states when an advantageous angle is caught (Mearsheimer, 2001).

What are the implications of this argument? By putting much lesser effort and capital compared to conventional offensive initiatives, cyber attacks may provide assailant parties with much higher returns (Valeriano et al., 2018; Watanabe, 2020). What is more, traditionally weaker states can vault power to challenge stronger states in cyberspace thanks to the low costs of organizing offensive actions (Pytlak and Mitchell, 2018). This means that cyberspace can be characterized as a leverage for traditionally weaker states and non-state actors, which would result in the redistribution of power (Langø, 2018; Singer and Friedman, 2014). On the other hand, it can be implied that states opt to use their cyber power in a defensive stance against non-state actors; however, when it comes to other states, it is always a feasible choice to abuse this power for an offensive action.

A neo-classical liberal approach may be proposed from different perspectives. As it is articulated by The White House (2000) "the Federal government alone cannot protect US critical infrastructures (…) For this Plan to succeed (The National Plan for Information Systems Protection), government and the private sector must work together in a partnership unlike any we have seen before (…)". Bendrath's perspective on the issue underpins this statement, taking such "partners" as private companies that may be of use in the establishment of a close private-public partnership (Bendrath, 2001). There hence exist more opportunities both for states and non-state actors to deepen cooperation in the cyberspace. However, one should also keep in mind that advancements in information technologies made the activities, especially organized cyber attacks, that take place on cyber realm much harder to surveil and charge the responsible party—or parties—in what follows. This intransparency paralyzes particularly the international organizations that specifically deal with monitoring state conflicts.

9. Declaration of Conflicting Interests

The author reports that there are no competing interests to declare.

10. Funding

No funding is provided to this study.

11. ORCID iD

Ahmet Selçuk Arslan

12. Data Availability Statement

The datasets and the code scripts used in this study are available at the link https://figshare.com/projects/Neorealist_Analysis_of_Security_Dilemma_in_Cyberspace_A_Quantitative_Study/163576 for replication purposes.

13. Ethical Approval

This article does not contain any studies with human participants performed by the author.

14. Informed Consent

This article does not contain any studies with human participants performed by the author.

15. References

Adams J (2001) Virtual Defense. *Foreign Affairs* 80(3): 98–112.

Azmi R, Tibben W and Than Win K (2016) Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. In: *Australasian Conference on Information Systems*, Wollongong, 2016.

Baezner M and Robin P (2017) *Hotspot Analysis: Stuxnet*. Center for Security Studies (CSS), ETH Zürich, Zürich.

Bendrath R (2001) The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information & Security: An International Journal* 7: 80–103. DOI: http://dx.doi.org/10.11610/isij.0705.

Choucri N (2012a) New Challenges to International Relations Theory and Policy. In: *Cyberpolitics in International Relations*. Cambridge, MA 02142: The MIT Press, p. 4.

Choucri N (2012b) The International System: Cyber Conflicts and Threats to Security. In: *Cyberpolitics in International Relations*. The MIT Press, pp. 125–154.

Choucri N (2012c) Theory Matters in International Relations. In: *Cyberpolitics in International Relations*. Cambridge, Massachusetts: The MIT Press, pp. 25–48.

Clark D, Berson T and Lin HS (2014a) *At the Nexus of Cybersecurity and Public Policy*. Computer Science and Telecommunications Board. National Research Council, Washington DC: The National Academies Press.

Clark D, Berson T and Lin HS (2014b) *At the Nexus of Cybersecurity and Public Policy*. Computer Science and Telecommunications Board. National Research Council, Washington DC: The National Academies Press.

Council on Foreign Relations (2023) Cyber Operations Tracker. Available at: https://www.cfr.org/cyber-operations/ (accessed 11 April 2023).

Creese S, Dutton WH and Esteve-González P (2021) The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and Ubiquitous Computing* 25(5): 941–955. DOI: 10.1007/s00779-021-01569-6.

Dartnell M (2003) Weapons of mass instruction: Web activism and the transformation of global security. *Millennium* 32(3): 477–499.

Denning D (2001) Activism, hacktivism, and cyberterrorism: The internet as a tool for influencing foreign policy. In: J. Arquilla DR (ed.) *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: Rand Corporation, pp. 239–288.

Dewar RS (2018) *National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1*. Zürich. Available at: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports_National_Cybersecurity_and_Cyberdefense_Policy_Snapshots_Collection_1.pdf (accessed 21 March 2023).

Drezner DW (2019) Technological change and international relations. *International Relations* 33(2). SAGE Publications Ltd: 286–303. DOI: 10.1177/0047117819834629.

Dunn Cavelty M (2008) *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.

Dunn Cavelty M and Wenger A (2020) Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy* 41(1). Routledge: 5–32. DOI: 10.1080/13523260.2019.1678855.

Dutton WH, Creese S, Shillair R, et al. (2019) Cybersecurity Capacity: Does It Matter? *Journal of Information Policy* 9: 280–306. DOI: 10.5325/jinfopoli.9.2019.0280.

Eriksson J and Giacomello G (2006) The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review* 27(3): 221–244. DOI: 10.1177/0192512106064462.

GCSCC (2021) *Cybersecurity Capacity Maturity Model for Nations (CMM)*.

GCSCC and CICTE (2020) *Cybersecurity Capacity Review: Federative Republic of Brazil*.

Glaser CL and Kaufmann C (1998) What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics). *International Security* 22(4).

Greathouse CB (2014) Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? In: Kremer J-F and Müller B (eds) *Cyberspace and International Relations: Theory, Prospects and Challenges*. New York: Springer Heidelberg, pp. 21–40.

Herz J (1951) *Political Realism and Political Idealism: A Study in Theories and Realities*. Chicago: University of Chicago Press.

Inkster N (2010) China in cyberspace. *Survival* 52(4): 55–66. DOI: 10.1080/00396338.2010.506820.

Jervis R (1978) Cooperation under the Security Dilemma. *World Politics* 30(2): 167–214. DOI: 10.2307/2009958.

Joseph J (2014) Realism and Neorealism in International Relations Theory. In: *The Encyclopedia of Political Thought*. Wiley, pp. 3142–3151. DOI: 10.1002/9781118474396.wbept0864.

Kassab HS (2014) In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In: Kremer J-F and Müller B (eds) *Cyberspace and International Relations: Theory, Prospects and Challenges*, pp. 59–76.

Kiggins RD (2014) US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. In: Kremer J-F and Müller B (eds) *Cyberspace and International Relations: Theory, Prospects and Challenges*. 1st ed. Heidelberg: Springer Berlin, pp. 161–180.

Kremer J-F and Müller B (2014) SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World. In: Kremer J-F and Müller B (eds) *Cyberspace and International Relations: Theory, Prospects and Challenges*. New York: Springer Heidelberg, pp. 41–58.

Langø H-I (2018) Competing academic approaches to cyber security. In: Friis K and Ringsmose J (eds) *Conflict in Cyber Space: Theoretical, Strategic and Legal Pespectives*. 1st ed. Routledge, pp. 23–42.

Luiijf E (2012) Understanding Cyber Threats and Vulnerabilities. In: Lopez J, Setola R, and Wolthusen SD (eds) *Lecture Notes in Computer Science*. Berlin, Heidelberg: Springer, pp. 52–67.

Luiijf E, Besseling K and Graaf P De (2013) Nineteen national cyber security strategies. *International Journal of Critical Infrastructures* 9(1/2): 3. DOI: 10.1504/IJCIS.2013.051608.

Lynn III WJ (2010) Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs* 89(5): 97–108. Available at: http://www.jstor.org/stable/20788647 (accessed 15 March 2023).

Mearsheimer JJ (2001) *The Tragedy of Great Power Politics*. W.W. Norton & Company.

Mohee A (2022) A Realistic Analysis of the Stuxnet Cyber-attack. *APSA Preprints*.

Morgan P (2007) Security in International Politics: Traditional Approaches. In: Collins A (ed.) *Contemporary Security Studies*. Oxford University Press, pp. 13–33.

Nakashima N (2015) Cyber chief: Efforts to deter attacks against the U.S. are not working. *The Washington Post*, 19 March. Available at: https://www.washingtonpost.com/world/national-security/head-of-cyber-command-us-may-need-to-boost-offensive-cyber-powers/2015/03/19/1ad79a34-ce4e-11e4-a2a7-9517a3a70506_story.html (accessed 15 March 2023).

Nye Jr JS (2022) The End of Cyber-Anarchy?: How to Build a New Digital Order. *Foreign Affairs* 101(1): 32–43.

O'Hanlon ME (2018) *The role of AI in future warfare*. 29 November. Available at: https://www.brookings.edu/series/a-blueprint-for-the-future-of-ai/ (accessed 15 March 2023).

Pytlak A and Mitchell GE (2018) Power, rivalry and cyber conflict: an empirical analysis. In: Friis K and Ringsmose J (eds) *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives*. 1st ed. Routledge.

Quester GH (2002) *Offense and Defense in the International System* (ed. J Wiley). 3rd ed. Transaction Publishers.

Rid T (2013) *Cyber War Will Not Take Place*. London: C. Hurst & Co.

Schmitt MN and Watts S (2016) Beyond State-Centrism: International Law and Non-state Actors in Cyberspace. *Journal of Conflict and Security Law* 21(3): 595–611. DOI: 10.1093/jcsl/krw019.

Shaheen S (2014) Offense–Defense Balance in Cyber Warfare. In: Kremer J-F and Müller B (eds) *Cyberspace and International Relations: Theory, Prospects and Challenges*. Springer, pp. 77–94. DOI: 10.1007/978-3-642-37481-4.

Singer PW and Friedman A (2014) Does the Cybersecurity World Favor the Weak or the Strong? In: *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press, pp. 150–152.

Slayton R (2017) What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security* 41(3). MIT Press Journals: 72–109. DOI: 10.1162/ISEC_a_00267.

Steed D (2011) Cyber power and strategy: So what? *Infinity Journal* 1(2): 21–24.

The Guardian (2017) How Russia used social media to divide Americans. *The Guardian*, 14 October. Available at: https://www.theguardian.com/us-news/2017/oct/14/russia-us-politics-social-media-facebook (accessed 7 April 2023).

The White House (2000) *Critical Infrastructure Protection: National Plan for Information Systems Protection*. Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwig7Nj78Or9AhUKQfEDHdGeAaMQFnoECAsQAQ&url=https%3A%2F%2Firp.fas.org%2Foffdocs%2Fpdd%2FCIP-plan.pdf&usg=AOvVaw07kdSZzlBurXBCEVStmZWd (accessed 20 March 2023).

The White House (2011) *International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*. May. Washington, D.C.

The White House (2023) *National Cybersecurity Strategy*. 1 March. Washington, D.C.

Tumkevič A (2019) *Potential of International Cooperation and Conflict in Cyberspace*. Doctoral Dissertation. Vilnius University, Lithuania. Available at: www.vu.lt/lt/naujienos/ivykiu-kalendorius.

USDOE (2022) *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*. October. Washington, D.C.

Valeriano B, Jensen BM and Maness RC (2018) *Cyber Strategy: The Evolving Character of Power and Coercion*. New York, NY: Oxford University Press.

V-Dem Coders (2023) Varieties of Democracy (V-Dem) Project. DOI: https://doi.org/10.23696/vdemds22.

Waltz K (1979) *Theory of International Politics*. Addison-Wesley Publishing Company.

Watanabe S (2020) States' Capacity Building for Cybersecurity: An IR Approach. In: *Human-Centric Computing in a Data-Driven Society. HCC 2020. IFIP Advances in Information and Communication Technology, vol 590* (eds D Kreps, T Komukai, T V. Gopal, et al.), 10 November 2020. Springer, Cham. DOI: 10.1007/978-3-030-62803-1_18.