

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 urged IR academia to account for state behaviour in cyberspace; one is the increasing volume of cyber attacks, and the other is the raising scale of damage induced by these attacks. This has brought a series of initiatives to appeal to the grand theories of IR so as to scrutinize state behaviour in depth in terms of securitization and militarization of the cyberspace. Subscribing to the same pattern of endeavor, this work intends to contribute to IR academia by putting forth a neorealist analysis of state behaviour in cyberspace by relying on quantitative methods. The analysis conducted by using a dataset consisting of 8,991 samples indicates that as states build more cyber security capacity, they become more tended to execute disruptive actions against other states in the cyberspace. Even after reinforcing the model with three additional control variables, the model yielded highly statistically important results.

2. Keywords

realism; neorealism; security dilemma; cyberpolitics; cyberspace

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; Dunn Cavelty & Wenger, 2020). Two crucial factors urged IR academia to account for state behaviour in cyberspace; one is the increasing volume of cyber attacks in recent years, and the other is the raising scale of damage induced by these attacks. These developments made states

more sensitive and demanding on the issues pertaining cyber security, leading them to establish their own peculiar national cyber security strategies (NCSS) (Luijckx et al., 2013). Though not endorsed by all, there is a wide-ranging implicative consensus reached upon the fact 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. In spite of the malignant outcomes of cyber attacks for states, there exist considerable amount of scholarly work that indicate the inappropriateness of the cyberspace to be accounted by the theories of IR. On the other hand, as of today, majority of the works that specifically deal with cyberspace politics achieved to yield empirical findings on state behaviour in cyber venues. Yet, the literature is having a wide gap as of today when it comes to provide this area of issue with a theoretical perspective anchored in an empirical quantitative analysis conducted by using historical data. Therefore, this work strives for bringing a theoretical framework on cyber politics by applying the concept of "security dilemma" on states' endeavor in pursuit of the militarization and the securitization of cyberspace (Mehmetcik, 2014). 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 "the state's cyber security capacity" as the independent variable, and "the state's dissemination of false information in foreign countries" as the dependent variable. The study relies purely on quantitative methods to justify the hypothesis. I compiled an 8,991 sample-sized dataset and produced five linear regression models in total, one of which is multivariate and the other four is bivariate. The multivariate model included three additional control variables to reinforce the reliability of the results, which is why I took it as my main model to test my hypothesis.

4. Previous relevant work

Back into the starting of the 21st century, several attempts were made to scrutinize and explain the relationship between state security and cyber medium to which (Bendrath, 2001) was an example, arguing that sustaining a stable and effective cyber security policy would be challenging for states particularly under liberal order in which infrastructure providers consist mostly of private companies. Nonetheless, this and such works either remained shallow in terms of providing a theoretical framework on security, or their remarkings 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 in the sense that the very existence of the term "cyber war" or "cyber warfare" has always been controversial. I would prefer to dichotomize these type 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 venues may have real-world implications, however, their results cannot be devastating 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 put his work on liberal line. 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), propoganda, identity theft, sabotage, and so forth (Choucri, 2012b; Denning, 2001; Greathouse, 2014; Inkster, 2010; Kassab, 2014; Kremer & Müller, 2014; Luiijf, 2012; Steed, 2011). I therefore point out that main inference that should be taken from such works is that there is no debate over whether cyber world facilitates such malignant actions; the main point of controversy is *to what extend* states bear to go for extraordinary offensive measures against one another as a consequence of these actions.

Such attempts were followed by highly suspicious accounts 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 & Giacomello, 2006). Going on a deeper level, I want to point out one velied aspect in the work of Eriksson & Giacomello (2006); I catch an implicit sight that they particularly draw attention on the undeniable and considerable amount of impacts of non-state actors in cyber venues. Therefore, I concluded from their work 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, which hold, in some cases, more power even than states. What counts as “power” in the cyber realm is a blurry issue, though; if it is counted as capacity to influence, Kremer & 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”.

Validity of such accounts has and had been challenged by a great number of works published in the last decade. 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 & Robin, 2017), Mohee (2022) concludes that anarchical nature of cyberspace makes offensive incentives more tempting, and cyber capabilites of states contribute to their survival. This is still a matter of big debate among scholars and is commonly accounted by

referring to the offense-defense theory of Robert Jervis (Jervis, 1978; Glaser & Kaufmann, 1998; Quester, 2002; Slayton, 2017). Although a consensus yet to be reached, most of scholarly works point out that developments in cyber technologies appreciate offensive actions. As indicated by Shaheen (2014), utilization of cyber weapons mostly for offensive actions but not for defensive purposes would tilt the offense-defense balance in favor of aggression, resulting in the destabilization of the international security system. Even though this study does not consider offense-defense theory as its central 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 forementioned 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 exists 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. On the one hand, no concessions are to be given on the idea reached by the realist consensus that both physical safety and autonomy are the compulsory elements of security, however, some realists may or may not attribute less importance on the “autonomy” and the “development”. Overlooking the developmental aspect may result in bitter consequences for a state 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 raised the attributed importance and precedence on cyber security, vaulting its degree of severity to national security level (Dewar, 2018). Cyber security, hence, is not 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 indeniability of the developmental aspect of security in the realist school of thought.

One foremost and identical characteristic of cyberspace that it shares with realist assumption of real world political system is its anarchical structure (Adams, 2001; Choucri, 2012c; Kiggins, 2014; Nye Jr, 2022), lack of an upper authority above states. One crucial point I intend to argue on is that 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, state is just a virtual being seen in cyberspace among other actors, such as hackers, other cyber terrorist groups and sometimes even NGOs, against whom its chief purpose is maintaining its security and existence in the realm. One may hence postulate that in a space where non-state actors dominates much of the acts of aggression, which is called “cyber attack” in cyberspace, states have no choice but focus on ensuring their own “survival” in the realm by taking advantage of the means called “cyber security”, which is possible 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 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)¹.

This postulation brings forth the question that how—or simply can—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. This means that technological innovations made by a state to improve its level of development in cyber technologies also increase its capacity to use these technologies in a disruptive manner, threatening internal and/or external security of the victim. Therefore, taking all the aforementioned arguments in this study so far into consideration, I hypothesize that raise in the cyber security capacity of states increases the tendency of the utilization of cyber power in a disruptive manner. I took states’ capability to disseminate false information in foreign countries as the action of disruption to use in my analysis.

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.

H_α = Raise in the cyber security capacity of states increases the tendency of the utilization of cyber power in a disruptive manner.

6. Data and Method

As mentioned in the previous section, my independent variable is government cyber security capacity, and dependent variable is dissemination of false information abroad. Data regarding these variables are taken from Varieties of Democracy Project (V-Dem) version 13 (V-Dem Coders, 2023). As stated by the respective coders preparing these data, scores for all countries are scaled to interval by the measurement model, which were ordinal in initial form. I took the scores for each individual country in the dataset between 1970 and 2022. Any missing data were replaced by the mean value of the corresponding column (variable). In total, I

¹ See Table 1.1 in; Choucri, N. (2012a). New Challenges to International Relations Theory and Policy. In Cyberpolitics in International Relations (p. 4). The MIT Press.

reached an adequate amount of sample size (8,991) to conduct a consistent analysis. I used OLS (linear) regression model in my analysis as my dependent variable is a continious measure.

Three additional control variables beside the independent variable were added in order to reinforce the consistency and the reliability of the analysis, which are taken from the same source, V-Dem project. These are defamation protection, government internet filtering capacity, and government capacity to regulate online content, all of which correlate with the dependent variable. Measurements applied on the independent and the dependent variables are also applied on the control variables in the same way. So as to provide a more reliable framework, four additional bivariate models were created for each of the control variables and the independent variable. Adding the multivariate model to these, in which all control variables and the independent variable involved in the calculation altogether, a regression table consisting of five linear models in total is produced. I used the language R to make all these operations and to create a regression plot suiting the results. The dataset I compiled after all these steps lacked the value “0” in the following variables: Dissemination of False Information Abroad, Defamation Protection, Internet Filtering Capacity, Capacity to Regulate Online Content. I therefore strived for reaching more optimal equations by subtracting the least value in each column (variables) from the all values in the each individual cell in the corresponding column.

7. Results

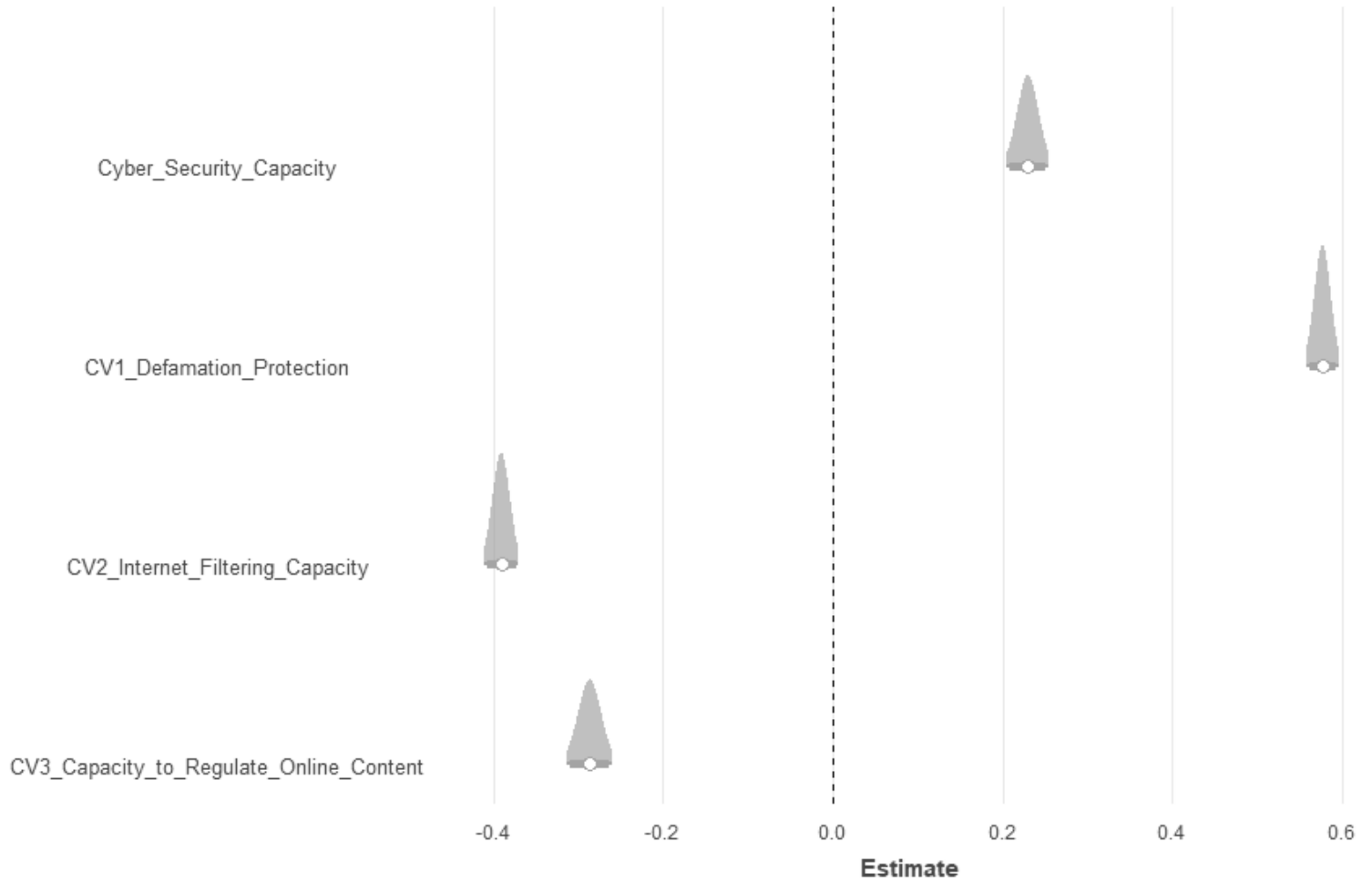
Table 1 and Figure 1 indicate the results of the analysis.

Table 1: OLS Regression Results

	Dependent variable:				
	Dissemination of False Information Abroad				
	(1)	(2)	(3)	(4)	(5)
Cyber Security Capacity	0.048*** (0.011)				0.230*** (0.013)
Defamation Protection (Control Variable)		0.570*** (0.010)			0.578*** (0.010)
Internet Filtering Capacity (Control Variable)			-0.395*** (0.010)		-0.391*** (0.010)
Capacity to Regulate Online Content (Control Variable)				-0.200*** (0.011)	-0.287*** (0.014)
Constant	0.543*** (0.010)	0.490*** (0.008)	0.494*** (0.009)	0.565*** (0.009)	0.521*** (0.008)
Observations	8,991	8,991	8,991	8,991	8,991
R²	0.002	0.254	0.139	0.035	0.455
Adjusted R²	0.002	0.254	0.139	0.034	0.455
Residual Std. Error	0.898 (df = 8989)	0.776 (df = 8989)	0.834 (df = 8989)	0.883 (df = 8989)	0.663 (df = 8986)
F Statistic	20.379*** (df = 1; 8989)	3,065.702*** (df = 1; 8989)	1,447.645*** (df = 1; 8989)	321.709*** (df = 1; 8989)	1,877.847*** (df = 4; 8986)

*p<0.1; **p<0.05; ***p<0.01

Figure 1: Regression Plot



In spite of the fact that each individual model yielded statistically important results, I took the model 5, in which I included all variables—including controls—to make a multivariate calculation, as the main model to test my hypothesis. The independent variable, which is the cyber security capacity of a state, showed highly statistically important result by falling below $P < 0.01$ threshold along with the other control variables. On the other hand, whilst cyber security capacity and defamation protection are found to have a positive-sided effect with the dependent variable, internet filtering capacity and capacity to regulate online content are found to have a negative-sided effect. This meant, in simpler terms, that increasing cyber security capacity also leads an increase in dissemination of false information abroad. The equations for each of the models are as follows;

First model, bivariate (Dissemination of False Information ~ Cyber Security Capacity):

$$\text{Dissemination of False Information} = \beta_0 + \beta_1 \text{Cyber Security Capacity} + \varepsilon$$

=

$$\text{Dissemination of False Information} = 0.543 + 0.048 + 0.898$$

Second model, bivariate (Dissemination of False Information ~ Defamation Protection):

$$\begin{aligned} \text{Dissemination of False Information} &= \beta_0 + \beta_1 \text{Defamation Protection} + \varepsilon \\ &= \\ \text{Dissemination of False Information} &= 0.490 + 0.570 + 0.776 \end{aligned}$$

Third model, bivariate (Dissemination of False Information ~ Internet Filtering Capacity):

$$\begin{aligned} \text{Dissemination of False Information} &= \beta_0 + \beta_1 \text{Internet Filtering Capacity} + \varepsilon \\ &= \\ \text{Dissemination of False Information} &= 0.494 + (-0.395) + 0.834 \end{aligned}$$

Fourth model, bivariate (Dissemination of False Information ~ Capacity to Regulate Online Content):

$$\begin{aligned} \text{Dissemination of False Information} &= \beta_0 + \beta_1 \text{Capacity to Regulate Online Content} + \varepsilon \\ &= \\ \text{Dissemination of False Information} &= 0.565 + (-0.200) + 0.883 \end{aligned}$$

Fifth model, multivariate (Dissemination of False Information ~ Cyber Security Capacity, Defamation Protection, Internet Filtering Capacity, Capacity to Regulate Online Content):

$$\begin{aligned} \text{Dissemination of False Information} &= \beta_0 + \beta_1 \text{Cyber Security Capacity} + \beta_2 \text{Defamation Protection} \\ &\quad + \beta_3 \text{Internet Filtering Capacity} + \beta_4 \text{Capacity to Regulate Online Content} + \varepsilon \\ &= \\ \text{Dissemination of False Information} &= 0.521 + 0.230 + 0.578 + (-0.391) + (-0.287) + 0.663 \end{aligned}$$

Taking all aforementioned calculations and inferences to consideration, the null hypothesis (H_0) is successfully rejected in favour of the alternative hypothesis (H_a); executing disruptive actions in the cyberspace becomes a more common practice for a country when its cyber security capacity raises.

8. Discussion and Conclusion

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 realist school of thought in order to ascribe explanations on state behaviour and foreign policy in 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 realist line of neorealism, indicating that states commonly tend to see cyber capacity building no different that "cyber power building" which is to 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 & 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 & 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, but when it comes to other states, it is always a viable choice to abuse this power for an offensive action.

A neo-classical realist approach can be made from different facades. 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 which are used for establishing 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 my 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. “When a nation tests a missile, the world knows almost immediately; when a nation constructs physical facilities for nuclear weapon development, other states or IOs can physically observe this and monitor it. However, when a nation tests a piece of malware, there is little to no way of knowing; when a nation begins ramping up their cyber capability, this goes unknown until execution of sophisticated attacks, or until malware is attributed to that state actor.” (Tischio, 2020).


9. Declaration of Conflicting Interests

The author reports 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 dataset and the code script used in this study is available at the link https://figshare.com/projects/Neorealist_Analysis_of_Security_Dilemma_in_Cyberspace_A_Quantitative_Study/163576 for replication purposes.

13. References

- Adams, J. (2001). Virtual Defense. *Foreign Affairs*, 80(3), 98.
- Azmi, R., Tibben, W., & Than Win, K. (2016). Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy. *Australasian Conference on Information Systems*.
- Baezner, M., & Robin, P. (2017). *Hotspot Analysis: Stuxnet*.
- Bendrath, R. (2001). The Cyberwar Debate: Perception and Politics in US Critical Infrastructure Protection. *Information & Security: An International Journal*, 7, 80–103.
<https://doi.org/http://dx.doi.org/10.11610/isij.0705>

- Choucri, N. (2012a). New Challenges to International Relations Theory and Policy. In *Cyberpolitics in International Relations* (p. 4). The MIT Press.
- Choucri, N. (2012b). The International System: Cyber Conflicts and Threats to Security. In *Cyberpolitics in International Relations* (pp. 125–154). The MIT Press.
- Choucri, N. (2012c). Theory Matters in International Relations. In *Cyberpolitics in International Relations* (pp. 25–48). The MIT Press.
- 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 D. R. J. Arquilla (Ed.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Rand Corporation.
- Dewar, R. S. (Ed.). (2018). *National Cybersecurity and Cyberdefense Policy Snapshots: Collection 1*. 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
- Drezner, D. W. (2019). Technological change and international relations. *International Relations*, 33(2), 286–303. <https://doi.org/10.1177/0047117819834629>
- Dunn Cavelty, M. (2008). *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*. Routledge.
- Dunn Cavelty, M., & Wenger, A. (2020). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), 5–32. <https://doi.org/10.1080/13523260.2019.1678855>
- Eriksson, J., & Giacomello, G. (2006). The information revolution, security, and international relations: (IR)relevant theory? *International Political Science Review*, 27(3), 221–244. <https://doi.org/10.1177/0192512106064462>
- Glaser, C. L., & Kaufmann, C. (1998). What is the offense-defense balance and can we measure it? (Offense, Defense, and International Politics). *International Security*, 22(4).
- Greathouse, C. B. (2014). Cyber War and Strategic Thought: Do the Classic Theorists Still Matter? In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 21–40). Springer Heidelberg.
- Inkster, N. (2010). China in cyberspace. *Survival*, 52(4), 55–66. <https://doi.org/10.1080/00396338.2010.506820>

- Jervis, R. (1978). Cooperation Under the Security Dilemma. *World Politics*, 30(2), 167–214. <http://www.jstor.org/stable/2009958?origin=JSTOR-pdf>
- Kassab, H. S. (2014). In Search of Cyber Stability: International Relations, Mutually Assured Destruction and the Age of Cyber Warfare. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 59–76).
- Kiggins, R. D. (2014). US Leadership in Cyberspace: Transnational Cyber Security and Global Governance. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (1st ed., pp. 161–180). Springer Berlin.
- Kremer, J.-F., & Müller, B. (2014). SAM: A Framework to Understand Emerging Challenges to States in an Interconnected World. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 41–58). Springer Heidelberg.
- Langø, H.-I. (2018). Competing academic approaches to cyber security. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, Strategic and Legal Perspectives* (1st ed., pp. 23–42). Routledge.
- Luijff, E. (2012). Understanding Cyber Threats and Vulnerabilities. In J. Lopez, R. Setola, & S. D. Wolthusen (Eds.), *Lecture Notes in Computer Science* (Vol. 7130, pp. 52–67). Springer.
- Luijff, E., Besseling, K., & Graaf, P. De. (2013). Nineteen national cyber security strategies. *International Journal of Critical Infrastructures*, 9(1/2), 3. <https://doi.org/10.1504/IJCIS.2013.051608>
- Lynn III, W. J. (2010). Defending a New Domain: The Pentagon's Cyberstrategy. *Foreign Affairs*, 89(5), 97–108. <http://www.jstor.org/stable/20788647>
- Mearsheimer, J. J. (2001). *The Tragedy of Great Power Politics*. W.W. Norton & Company.
- Mehmetcik, H. (2014). A New Way of Conducting War: Cyberwar, Is That Real? In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 125–140).
- Mohee, A. (2022). A Realistic Analysis of the Stuxnet Cyber-attack. *APSA Preprints*.
- Morgan, P. (2007). Security in International Politics: Traditional Approaches. In A. Collins (Ed.), *Contemporary Security Studies* (pp. 13–33). Oxford University Press.
- Nakashima, N. (2015, March 19). Cyber chief: Efforts to deter attacks against the U.S. are not working. *The Washington Post*. 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
- Nye Jr, J. S. (2022). The End of Cyber-Anarchy?: How to Build a New Digital Order. *Foreign Affairs*, 101(1), 32–43.

- O'Hanlon, M. E. (2018). *The role of AI in future warfare*. <https://www.brookings.edu/series/a-blueprint-for-the-future-of-ai/>
- Pytlak, A., & Mitchell, G. E. (2018). Power, rivalry and cyber conflict: an empirical analysis. In K. Friis & J. Ringsmose (Eds.), *Conflict in Cyber Space: Theoretical, strategic and legal perspectives* (1st ed.). Routledge.
- Quester, G. H. (2002). *Offense and Defense in the International System* (J. Wiley, Ed.; 3rd ed.). Transaction Publishers.
- Rid, T. (2013). *Cyber War Will Not Take Place*. C. Hurst & Co.
- Shaheen, S. (2014). Offense–Defense Balance in Cyber Warfare. In J.-F. Kremer & B. Müller (Eds.), *Cyberspace and International Relations: Theory, Prospects and Challenges* (pp. 77–94). Springer. <https://doi.org/10.1007/978-3-642-37481-4>
- Singer, P. W., & Friedman, A. (2014). Does the Cybersecurity World Favor the Weak or the Strong? In *Cybersecurity and cyberwar: What everyone needs to know* (pp. 150–152). Oxford University Press.
- Slayton, R. (2017). What is the cyber offense-defense balance? Conceptions, causes, and assessment. *International Security*, 41(3), 72–109. https://doi.org/10.1162/ISEC_a_00267
- Steed, D. (2011). Cyber power and strategy: So what? *Infinity Journal*, 1(2), 21–24.
- The White House. (2000). *Critical Infrastructure Protection: National Plan for Information Systems Protection*. <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>
- Tischio, R. M. (2020). *Hacking Nation-State Relationships: Exploiting the Vulnerability of the Liberal International Order* [Senior Thesis, Fordham University]. https://research.library.fordham.edu/international_senior/47
- Tumkevič, A. (2019). *Potential of International Cooperation and Conflict in Cyberspace* [Doctoral Dissertation, Vilnius University]. www.vu.lt/lt/naujienos/ivykiu-kalendarius
- Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.
- V-Dem Coders. (2023). *Varieties of Democracy (V-Dem) Project*. V-Dem Dataset V13. <https://doi.org/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 D. Kreps, T. Komukai, T. V. Gopal, & K. Ishii (Eds.), *Human-Centric Computing in a Data-Driven Society. HCC 2020. IFIP Advances in Information and Communication Technology, vol 590*. Springer, Cham. https://doi.org/10.1007/978-3-030-62803-1_18