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

Could countries' cyber security capacity-building result in the emergence of a security dilemma in cyberspace? This work seeks to answer this question by bringing a theoretical framework through a neorealist perspective. The author argues that neorealism remains a relevant theory for explaining state behaviour in cyberspace by providing a quantitative backbone to the theoretical discussions on the subject. The analysis made by deploying a negative binomial regression incorporating fixed effects on panel data suggests that as countries build more cyber security capacity, it is more likely for them to be targeted by cyber attacks. Robustness checks of the findings were subsequently performed using logistic regression with fixed effects on panel data by mutating the dependent variable into binary format, which enhanced the validity of the results computed by the negative binomial model.

2. Keywords

realism; neorealism; security dilemma; cyberpolitics; cyber security

3. Introduction

It comes as no surprise that the digital era has ushered cyberspace as the fifth domain of warfare almost for one and half decade, beside air, space, sea and land (Azmi et al., 2016), particularly due to the increasing volume of cyber attacks in recent years (USDOE, 2022) and the raising scale of damage induced by these attacks[1] (Dunn Cavelty & Wenger, 2020). This transformation has made countries more sensitive and

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

https://doi.org/10.33774/apsa-2023-ww2z-v10 **ORCID:** https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. **License:** CC BY 4.0

demanding on the issues pertaining cyber security, leading them to establish their own peculiar national cyber security strategies (NCSS) (Luiijf et al., 2013). Having engaged in cyber security capacity building, could countries' security-seeking behaviour result in the emergence of a security dilemma in cyberspace?

This work seeks to bring a theoretical framework to this question through a neorealist lens by focusing on the concept of 'security dilemma'. I argue that neorealism is still a relevant theory to explain *cyberpolitics*[2] of security in that neorealism's structural approach to international politics is particularly adept at explaining state behaviour in cyberspace. Taking cyber security capacity as the independent variable and the number of cyber attacks received as the dependent variable, I contend that as countries increase their cyber security capacity, they become more exposed to state-sponsored cyber attacks as a consequence of the security dilemma. What distinguishes this study from other relevant works in the literature in doing so is its quantitative methodological approach to the research question, particularly through the use of a negative binomial regression on longitudinal data ranging from 2005 to 2023. Robustness checks of the findings obtained from the negative binomial regression are subsequently performed using logistic regression on dummy data, which enhances the trustworthiness of the study's conclusions.

The following section (section four) provides a sketch of literature review on the subject. Section five lays the argumentative foundations for the logic behind adopting neorealism to cyberspace, and proposes the hypothesis of the study in what follows. Section six clarifies the methodological stance of the work and shares relevant information regarding the data used. Section seven interprets the results obtained by the data analysis, where I found statistically significant results regarding the hypothesis that 'as countries increase cyber security capacity, they receive more cyber attacks'. Section eight concludes the study, where I elaborate on the implications of the results obtained, suggestions for future research, and limitations of the study.

4. 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, while this and such works provide valuable insights, either they often do not offer a comprehensive theoretical framework on security issues, or their conclusions rely heavily on assumptions due to the lack of adequate empirical data of the time. It should also be noted that the very existence of 'cyber war' or 'cyber warfare' has always been controversial since there is nowhere to place these concepts in the conventional Clausewitzian definition of war. Clausewitz (1989) differentiates war from other types of conflicts in that it is resolved through bloodshed; this is the sole characteristic distinguishing it from other

[2] The term *cyberpolitics* is a recently coined term that combines two realities: those pertaining to politics, and those enabled by the uses of cyberspace (Choucri, 2012b).

conflicts, which does not align with the nature of cyber warfare. Nevertheless, it is possible to see in the academic literature that there are differing views regarding the existence of cyber warfare, with some works asserting its genuineness and others questioning it. On the one hand, according to Rid (2012) and other similar skeptic perspectives, malicious actions taken in cyberspace may have real-world implications and can be resolved before evolving into a large scale real-world war. Which is why their outcomes are not likely to be more devastating than conventional acts of violence, with war as a tangible action being unlikely to occur in cyberspace. And on the other, Stone (2013) and analogous research posit that cyber attacks can be deemed acts of war by virtue of their forceful and violent characteristics. It is nonetheless a fact 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, etc. (Choucri, 2012c; Denning, 2001; Greathouse, 2014; Inkster, 2010; Kassab, 2014; Kremer & Müller, 2014; Luiijf, 2012; Steed, 2011). I accordingly 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 are willing to engage in extraordinary offensive measures against one another as a retaliatory response to the damage caused by such malicious actions.

Further debate has arisen concerning the relevance of theoretical frameworks to cybersecurity issues, highlighting either a lacuna in or challenge for the theoretical constructs (Choucri, 2012a; Choucri & Goldsmith, 2012), or the inadequacies of grand international relations theories in elucidating state behaviour regarding security in cyberspace (Eriksson & Giacomello, 2006). A great number of works published in the last decade have been dedicated to exploring these propositions. Among these, the work of Tumkevič (2019) is particularly relevant, drawing attention to 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 addresses 'capacity building' in cyberspace and provides a more comprehensive framework by applying three theoretical approaches (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 robustness of these findings may be questioned if not supported by empirical data.

In his analysis on Stuxnet cyber attack incident[3] in 2010, 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 & Kaufmann, 1998; Jervis, 1978; Quester, 2002; Slayton, 2017). Although a consensus has yet to be reached, most scholarly works point out that developments in cyber technologies favour offensive actions (Drezner, 2019; Lynn III, 2010; Mohee, 2022; Nakashima, 2015;

[3] For more information on Stuxnet cyber attack, see Baezner, M., & Robin, P. (2017). Hotspot Analysis: Stuxnet. Center for Security Studies (CSS), ETH Zürich.

O'Hanlon, 2018). Reason to this is that cyber offensive capabilities are characterized to be 'force multipliers' with potentially high impact and low cost (Smeets, 2018). As indicated by Shaheen (2014), the utilization of cyber capabilities in offensive ways for such reasons 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 as its chief theory of explanation, it implicitly relates the adoption of defensive measures to offensive responses given by foreign countries, and how increasing capacity for the former may subsequently contribute to the emergence of the latter, triggering a vicious spiral.

One research deserves a special attention: the work of Pytlak and Mitchell (2018) aligns closely with the logical framework of this research in that they focus on quantitative measures to ascertain the drivers of cyber interactions among nations. Specifically, their findings suggest that nuclear capability of a state can be considered a motivator for cyber conflicts. However, as seen in other aforementioned studies, the majority of works that seek to bring a theoretical perspective on cyber security-related issues lack quantitative data analysis to reinforce their findings. This gap also hinders the improvement of existing theories, and the development of new theoretical perspectives. Therefore, this work aims to present a satisfactory realist point of view anchored in quantitative analysis using historical data to address the methodological gap in the literature.

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

Is it possible to take cyberspace as a political structure? In *Theory of International Politics*, Waltz (1979) attributes three elements to political structures: an ordering principle (anarchic or hierarchical), the character of the units (functionally alike or differentiated), and the distribution of capabilities. Waltz adds that two of these elements are constants of international system: the lack of an overarching authority above actors or units, which is anarchy, and the principle of self-help, meaning that all units remain functionally alike (Elman, 2012). However, one should note that these constants are not mutually exclusive elements, as it is the anarchy that induces the self-help system that holds different units and actors functionally alike in the motive of seeking survival. Whether cyberspace encapsulates the anarchical nature of real-world international political system is a recent debate among scholars, a considerable portion of whom identify anarchy as a pedestal feature of cyberspace identical to real-word international political structure (Adams, 2001; Choucri, 2012e; Kiggins, 2014; Nye, 2022). This is because states are considered virtual units in cyberspace among other actors, such as hackers, other cyber terrorist groups, and sometimes NGOs, each of which have to look for themselves by leveraging the means holistically known as *cyber security* and thus, accomplishing the ultimate goal of survival in the realm.

A question mark arises at this point in that why a state has to exhibit existence and care for its survival in cyberspace? Diving into the Gulf War of 1991 may provide us with a reasonable answer to this question. The conflict was characterized by military strategist and theorists as an unconventional way of putting military muscle on the ground, particularly by the US military, which cemented the use of kinetic force with information and communication technologies (ICTs). The war was therefore interpreted as the first of new generation of information age conflicts (Cavelty, 2013). This paved the way to the development of new military doctrines grounded on paralysing opponent's communication systems (Arquilla & Ronfeldt, 1993; Campen, 1992). These and such developments indicate the pivotal advantages of cyber technologies, which provides a country with an 'information edge' (Nye & Owens, 1996).

This leaves the distribution of capabilities the only variable in Waltz's framework for categorizing political structures of systems as either multipolar or bipolar. The period during which Waltz authored his work was marked densely by cold war dynamics, which sheds light on why Waltz's discourse is limited to bipolar and multipolar systems in his work. The post-cold war era witnessed the expansion of Waltz's foundational ideas on systems into unipolar, bipolar, and multipolar ramifications[4]. If this systematic approach is to be examined within the scope of cyberspace in a political context, I contend, it is feasible to talk about a multipolar order. The chief reason to this is that advancements in ICTs have catalyzed a shift in the balance of power in cyberspace, increasingly favouring non-state actors in terms of power equation (Rowland et al., 2014) who, in some cases, now wield more power[5] than states themselves (Schmitt & Watts, 2016). This argument is buttressed by Dartnell (2003) with the following words: "(ICT provides) enormous opportunities for non-state actors and enhances the global profile of previously marginalised issues and movements". It also stands to reason that some inherent features of cyberspace afford non-state actors a greater degree of autonomous operational capacity. Particularly, these features are *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)[6].

Drawing upon the preceding arguments, one can delineate cyberspace as inherently political in structure based on Waltz's definition. Based on this postulation, this research brings forth the question that could security dilemma manifest in cyberspace in the light of the security understanding of states in cyberspace mentioned above? The possibility of dual-use of the capacity built for defensive purposes gives rise to the security dilemma (Herz, 1951; Jervis, 1978), agitating and thereby leading to *preventive* responses from other states (Badie et al., 2011). I hence argue that states with higher cyber security capacities may find themselves more likely to be targeted by cyber attacks.

$\boldsymbol{H_0}$ = *States with higher cyber security capacities are not more likely to be targeted by cyber attacks compared to those with lower cyber security capacities.*

[4] For an exceptional approach based on *nonpolarity*, see Haass, R. N. (2008). The Age of Nonpolarity. Foreign Affairs, 1–11.

[5] What counts as power in the cyber realm is a blurry issue, though. It may have to do with the capacity to destroy and disrupt, as seen in the aforementioned Gulf War example, as well as with the capacity to influence through "the direction of (public) opinion by either providing, shaping or withholding information" (Kremer & Müller, 2014).

[6] For the list identifying all characteristics of cyberspace, 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 .

H_a = *States with higher cyber security capacities are more likely to be targeted by cyber attacks compared to those with lower cyber security capacities.*

6. Research Design and Method

This study employs a correlational research strategy via deploying a quantitative approach to the research question by compiling and analysing existing datasets. It is correlational in that it seeks to identify a possible relationship between *cyber security capacity* (independent variable, abbreviated as 'IV'), and *cyber attacks received* (dependent variable, abbreviated as 'DV'). Since the research strives to test the theoretical proposition of the security dilemma, it is deductive and confirmatory in nature. These aspects collectively suggest that regression is arguably the best choice of statistical test for analysis, which excels specifically at exposing causal links between variables. Considering that the DV records the sum of the counts of cyber attacks that each country is exposed to on yearly basis, regression analysis via Poisson or Negative Binomial models is feasible as these models are tailored for discrete count data. Deciding between Poisson or negative binomial model is based on the difference between the mean and the variance of the DV. For my data, the mean of the DV is 0.3722, and the variance is 0.7278493. Considerable margin (0. 3556493) between these measures indicates overdispersion, which suggests the use of a negative binomial regression model for the data.

Data pertaining to the IV were derived from the 'government cyber security capacity' index of Varieties of Democracy Project (V-Dem) version 14 (Coppedge et al., 2024), with scores for each available country in the dataset recorded from 2005 to 2023. Data for the DV were sourced from the dataset created by the Council on Foreign Relations (2024), which records each known state-sponsored cyber attack between 2005 and 2023. The dataset I compiled from these repositories is organized longitudinally by taking country-years as the unit of observation, making it optimal for the use of panel data analysis techniques. Given that each country's inherent characteristics (which do not vary over time but might differ across countries) could influence the DV, controlling for all these time-invariant differences would facilitate focusing merely on the impacts of changes in cyber security capacity of each country over time. This rationale supports the use of fixed effects model to analyze the compiled panel data.

Four additional variables are added as controls. Three of these have to do with the interplay between political regimes and cyber incidents. I argue that autocracies and democracies each have their own peculiar political and governance models, which may manifest in diverse behaviour and response to cyber incidents. Take the following as an example; more authoritarian regimes might engage more in state-sponsored cyber activities both domestically and internationally. This could be, for instance, disseminating false information for regime propaganda and power consolidation. I hence include liberal democracy index, political corruption, and dissemination of false information abroad as control variables, with all data obtained from the V-Dem dataset (Coppedge et al., 2024). The last control variable is GDP per capita. Found by Kumar & Carley (2016), countries with higher GDP per capita are targeted more often by cyber attacks. The reason for this may be that wealthier nations with higher volumes of capital flows are seen lucrative targets for ransom demands and financial frauds. Therefore, it is logical to include GDP per capita as a control variable, with the data obtained from V-Dem.

Missing values were observed only in GDP per capita variable. The data initially tested for MCAR (missing completely at random) using 'naniar' package (Tierney & Cook, 2023), which returned a *p*-value of less than 0.05, meaning that missingness could not be attributed to MCAR. Attributing missingness to MAR (missing at random), multivariate imputation by chained equations (MICE) was subsequently employed to predict and fill the missing data. Consequently, the DV was converted into a dummy variable to perform a robustness check using logistic regression with fixed effects, 1 if the country in question received a cyber attack in the corresponding year, and 0 if not. The hypothesis was tested on both bivariate and multivariate bases. All procedures described in this section were implemented using R language. See Appendix A for explanatory information regarding variables in the dataset, and Appendix B for the results of robustness check.

7. Results

Table 1 indicate the numerical results of the analysis.

Table 1: Negative Binomial Models with Fixed Effects

	Model 1	Model 2	Model 3	Model 4
Intercept	0.944**	2.298***	5.014***	3.514***
	(0.305)	(0.454)	(0.611)	(0.683)
Hypothesis				
Cyber Security Capacity	1.021***	1.052***	0.901***	0.751***
	(0.087)	(0.087)	(0.089)	(0.095)
Controls				
Liberal Democracy Index		−2.757***	−4.628***	−2.052**
		(0.513)	(0.592)	(0.696)
Political Corruption			−3.492***	−2.578***
			(0.611)	(0.634)
Dissemination of False Information Abroad via Social Media				−0.475***
				(0.072)
GDP Per Capita				0.000***
				(0.000)
Dependent Variable:	Cyber Attacks Received			
Log Likelihood	−1587.609	−1572.686	−1556.540	−1521.138
AIC	3179.218	3151.372	3121.080	3054.276

***p < 0.001; **p < 0.01; *p < 0.05

Four models were created to test the hypothesis on both bivariate and multivariate bases. All variables (including controls) yielded highly statistically important results by falling below $p < 0.001$ threshold. 'Cyber Security Capacity' (IV) was found to have a positive-sided relationship with 'Cyber Attacks Received'

(DV) in all models. Whilst 'Liberal Democracy Index', 'Political Corruption', and 'Dissemination of False Information Abroad via Social Media' are found to have a negative association, 'GDP Per Capita' is found to have a positive association with the DV. These results indicate that as countries move away from liberal democracy and disseminate more false information abroad, they receive more cyber attacks. Moreover, as they get less corrupt and reach higher levels of GDP per capita, they receive more cyber attacks. And lastly, as cyber security capacity increases, countries receive more cyber attacks. The null hypothesis ($\boldsymbol{H_0}$) is successfully rejected in favour of the alternative hypothesis ($\boldsymbol{H_a}$); getting exposed to cyber attacks becomes a more common phenomenon for a country when its cyber security capacity raises. Robustness checks of the models were performed by logit models with fixed effects, which reinforced the credibility and reliability of the outcomes obtained through negative binomial regression models with fixed effects, enhancing the trustworthiness of the study's conclusions (see Appendix B).

8. Discussion and Conclusion

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 countries are also exposed to more cyber attacks as they build cyber security capacity. This results in a vicious *security dilemma*, which is one of the key tenets in the realist understanding of international politics, and which emerges as a consequence of the possibility of the dual-use of capacity (Herz, 1951; Jervis, 1978). 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 cyberspace as well.

Another issue is that by putting much lesser effort and capital compared to conventional offensive initiatives, cyber attacks may provide assailant parties with much higher returns (Smeets, 2018; 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).

From a theoretical point of view, while 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 approaches 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 cyberspace in the sense that cyberspace, 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 to allow the measurement of states' cyber security capacity using relevant techniques.

The concept of 'security' could be 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 (Choucri, 2012d; Dunn Cavelty, 2008). Therefore, I find fair to put forth the argument that emergence of cyber challenges cements the undeniability of the developmental aspect of security in the realist school of thought.

The process of cyber security capacity building does not solely rely on technical flourishment (Clark et al., 2014); managerial, social, legal, policy, and regulatory aspects of development are also considered the very components of this process (Clark et al., 2014; Creese et al., 2021; Dutton et al., 2019; GCSCC, 2021). 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 cyber security 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 cyberspace intact against domestic rival figures (GCSCC & CICTE, 2020; The White House, 2011, 2023). It is hence feasible to theoretically examine the impacts of certain relevant indicators, such as defamation protection, government internet filtering capacity and government capacity to regulate online content, in relation to the cyber security-capacity building initiatives of countries. It also deserves special attention to investigate the causal links between the control variables and their relationship to the DV used in this study. For instance, it is an interesting finding that countries with lower liberal democracy scores are subjected to more cyber attacks, while countries with higher levels of political corruption experience fewer.

This research is not free of limitations, of course. The existing literature provides academia with vast amounts of datasets to measure a given country's security capacity 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

https://doi.org/10.33774/apsa-2023-www2z-v10 **ORCID:** https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. **License:** CC BY 4.0

to examine available data that are suitable to be adapted on the dependent variable. Only available data I could reached was the cyber operations tracker of the Council of Foreign Relations, which is an open database and has its own limitations. First of these is the incompleteness of the data due to the reason that most private cyber security firms and state intelligence agencies biased towards classifying the complete data on state-sponsored cyber attacks on account of national security reasons and trade secrets. Second is the time it takes to identify the real initiator of the cyber attack in question, as it is highly probable that states masquerade as non-state actors during cyber operations. Third is the brevity of the time period that the dataset covers, encompassing the short period between 2005 and 2023. Further analysis conducted with more data recorded over a longer timeline may result in the refutation of the findings reached by this study.

9. ORCID iD

Ahmet Selçuk Arslan

10. Data Availability Statement

The datasets and the code script used for this study are available at the link https://dx.doi.org/10.6084/m9.figshare.25751796 for replication purposes.

11. References

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

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming! *Comparative Strategy*, *12*(2), 141–165.

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*.

Badie, B., Berg-Schlosser, D., & Morlino, L. (2011). Security Dilemma. In *International Encyclopedia of Political Science* (pp. 2390–2391). SAGE Publications, Inc. https://doi.org/10.4135/9781412994163

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

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

Campen, A. D. (Ed.). (1992). *The First Information War: The Story of Communications, Computers, and Intelligence Systems in the Persian Gulf War* (1st ed.). AFCEA International Press.

Cavelty, M. D. (2013). Cyber-security. In A. Collins (Ed.), *Contemporary Security Studies* (3rd ed., pp. 362–378). Oxford University Press.

Choucri, N. (2012a). Introduction. In *Cyberpolitics in International Relations* (p. 14). The MIT Press. https://doi.org/10.7551/mitpress/7736.003.0003

Choucri, N. (2012b). Introduction. In *Cyberpolitics in International Relations* (pp. 4–5). The MIT Press.

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

Choucri, N. (2012d). The International System: Cyber Conflicts and Threats to Security. In *Cyberpolitics in International Relations* (p. 126). The MIT Press.

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

Choucri, N., & Goldsmith, D. (2012). Lost in cyberspace: Harnessing the Internet, international relations, and global security. *Bulletin of the Atomic Scientists*, *68*(2), 70–77. https://doi.org/10.1177/0096340212438696

Clark, D., Berson, T., & Lin, H. S. (2014). *At the nexus of cybersecurity and public policy*. Computer Science and Telecommunications Board. National Research Council, Washington DC: The National Academies Press.

Clausewitz, C. von. (1989). *On War* (M. Howard & P. Paret, Eds.; p. 149). Princeton University Press.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Altman, D., Bernhard, M., Cornell, A., Fish, M. S., Gastaldi, L., Gjerløw, H., Glynn, A., God, A. G., Grahn, S., Hicken, A., Kinzelbach, K., Krusell, J., Marquardt, K. L., McMann, K., … Ziblatt, D. (2024). *V-Dem [Country-Year/Country-Date] Dataset v14* (14). Varieties of Democracy (V-Dem). https://doi.org/https://doi.org/10.23696/mcwt-fr58

Council on Foreign Relations. (2024). *Cyber Operations Tracker*. CFR. https://www.cfr.org/cyber-operations/

Creese, S., Dutton, W. H., & 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. https://doi.org/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 D. R. J. Arquilla (Ed.), *Networks and netwars: The future of terror, crime, and militancy* (pp. 239–288). Rand Corporation.

Dewar, R. S. (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

Dutton, W. H., Creese, S., Shillair, R., & Bada, M. (2019). Cybersecurity Capacity: Does It Matter? *Journal of Information Policy*, *9*, 280–306. https://doi.org/10.5325/jinfopoli.9.2019.0280

Elman, C. (2012). Neorealism: Waltz's Theory of International Politics. In P. D. Williams (Ed.), *Security Studies: An Introduction* (2nd ed., pp. 18–20). Routledge.

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

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

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

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.

Haass, R. N. (2008). The Age of Nonpolarity. *Foreign Affairs*, 1–11.

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

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. https://doi.org/10.2307/2009958

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

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.

Kumar, S., & Carley, K. M. (2016). Approaches to understanding the motivations behind cyber attacks. *2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, 307–309. https://doi.org/10.1109/ISI.2016.7745496

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

Luiijf, 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.

Luiijf, 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

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

Nye, J. S., & Owens, W. A. (1996). America's Information Edge. *Foreign Affairs*, 20–36.

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. (2012). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

Rowland, J., Rice, M., & Shenoi, S. (2014). The anatomy of a cyber power. *International Journal of Critical Infrastructure Protection*, *7*(1), 3–11. https://doi.org/10.1016/j.ijcip.2014.01.001

Schmitt, M. N., & Watts, S. (2016). Beyond State-Centrism: International Law and Non-state Actors in Cyberspace. *Journal of Conflict and Security Law*, *21*(3), 595–611. https://doi.org/10.1093/jcsl/krw019

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

Smeets, M. (2018). The Strategic Promise of Offensive Cyber Operations. *Strategic Studies Quarterly*, *12*(3), 90–113.

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

Stone, J. (2013). Cyber War Will Take Place! *Journal of Strategic Studies*, *36*(1), 101–108. https://doi.org/10.1080/01402390.2012.730485

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=2ahUKEwig7Nj78

Or9AhUKQfEDHdGeAaMQFnoECAsQAQ&url=https%3A%2F%2Firp.fas.org%2Foffdocs%2Fpdd%2FCIP-plan.pdf&usg=AOvVaw07kdSZzlBurXBCEVStmZWd

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

The White House. (2023). *National Cybersecurity Strategy*.

Tierney, N., & Cook, D. (2023). Expanding Tidy Data Principles to Facilitate Missing Data Exploration, Visualization and Assessment of Imputations. *Journal of Statistical Software*, *105*(7). https://doi.org/10.18637/jss.v105.i07

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

USDOE. (2022). *Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid*.

Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber Strategy: The Evolving Character of Power and Coercion*. Oxford University Press.

Waltz, K. N. (1979). *Theory of International Politics*.

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

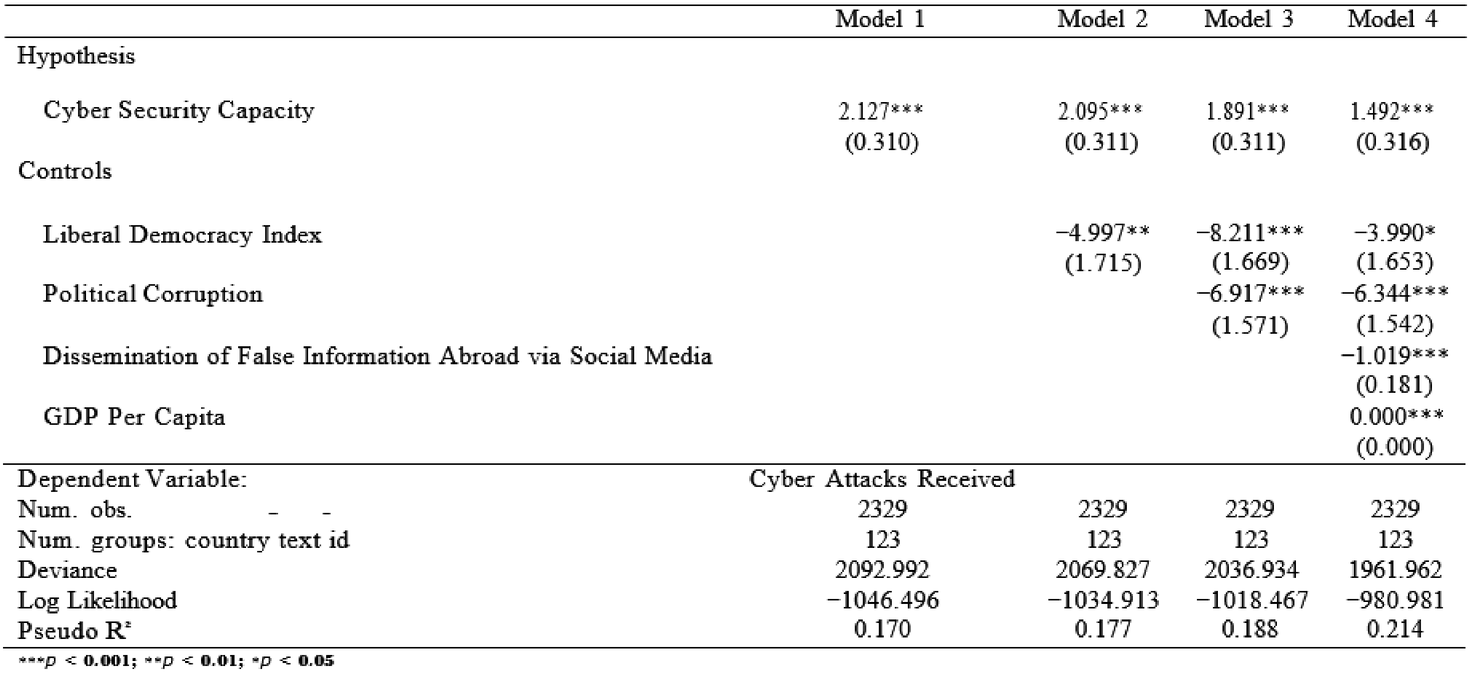
12. Appendices

Appendix A: Variable Information

Variable	Description	Scale
country_name	Name of the country in question.	N/A
country_text_id	Correlates of War (COW) code of the country in question in character format.	N/A
year	Corresponding year of the incident.	Discrete
attacks_received	Number of cyber attacks to which the country in question is exposed in the corresponding year. Data taken from the 'Cyber Operations Tracker' of the Council on Foreign Relations.	Discrete, count
Cyber_Security_Capacity	Numerical denotation of the cyber security capacity of the country in question in the corresponding year. Data taken from the 'Government cyber security capacity' indicator of the V-Dem project.	Interval, from low to high (0-1)
Liberal_Democracy_Index	Liberal democracy score of the country in question in the corresponding year. This index also takes electoral democracy score into account. Data taken from the 'Liberal Democracy Index' indicator of the V-Dem project.	Interval, from low to high (0-1)
Political_Corruption	Numerical denotation of the level of political corruption of the country in question in the corresponding year. Data taken from the 'Political corruption index' indicator of the V-Dem Project.	Interval, from low to high (0-1)
Dissemination_of_False_Information_Abroad	Numerical denotation of the frequency of disseminating misleading viewpoints or false information to influence citizens of other countries abroad. Data taken from the 'Government dissemination of false information abroad' indicator of the V-Dem Project.	Interval, from high to low (0-1)
GDP_Per_Cap	The sum of gross value added by all resident producers in the economy plus any product taxes. Data taken from the 'GDP Per Capita' indicator of the V-Dem Project.	Continuous

https://doi.org/10.33774/apsa-2023-www2z-v10 **ORCID:** https://orcid.org/0000-0001-8635-3402 Content not peer-reviewed by APSA. **License:** CC BY 4.0

Appendix B: Robustness Check with Logit Models



	Model 1	Model 2	Model 3	Model 4
Hypothesis				
Cyber Security Capacity	2.127*** (0.310)	2.095*** (0.311)	1.891*** (0.311)	1.492*** (0.316)
Controls				
Liberal Democracy Index		−4.997** (1.715)	−8.211*** (1.669)	−3.990* (1.653)
Political Corruption			−6.917*** (1.571)	−6.344*** (1.542)
Dissemination of False Information Abroad via Social Media				−1.019*** (0.181)
GDP Per Capita				0.000*** (0.000)
Dependent Variable:	Cyber Attacks Received			
Num. obs. – -	2329	2329	2329	2329
Num. groups: country text id	123	123	123	123
Deviance	2092.992	2069.827	2036.934	1961.962
Log Likelihood	−1046.496	−1034.913	−1018.467	−980.981
Pseudo R^2	0.170	0.177	0.188	0.214

***$p < 0.001$; **$p < 0.01$; *$p < 0.05$