KYIV SCHOOL OF ECONOMICS

PUBLIC POLICY AND GOVERNANCE MASTER'S PROGRAM

MASTER'S THESIS

# "HOW DOES THE SIZE OF THE STATE'S WINNING COALITION AFFECT ITS BEHAVIOUR IN CYBERSPACE?"

Student: Maksym Klovak
Research advisor: Anastasiia Vlasenko, PhD in Political Science

For obtaining an educational degree: Master's
in speciality: 281 Public Management and Administration

Kyiv 2026

CONTENTS

## ANNOTATION

Selectorate theory has not been tested regarding states' cyber aggression. This study answers the question: “How does the size of the state's winning coalition affect its behaviour in cyberspace?” Specifically, I analyse whether the size of the winning coalition predicts the frequency of state-backed cyber operations. I utilise the dataset of cyber incidents covering the years 2007 through 2020 and apply Negative Binomial and Zero-Inflated Negative Binomial regressions. The results show that broader winning-coalition regimes are associated with a lower frequency of unprovoked cyber operations originating from them. However, the winning coalition does not predict the targets of cyberattacks. Policy-makers could therefore use the winning coalition index as a screen for potential cyber threats.

Key words: selectorate theory, winning coalition, cyberspace, cyber operations, political regimes

Word count: 12787

## INTRODUCTION

The question of state aggression has been a focus of international relations scholarship for decades. Meanwhile, the expansion of the Internet has established cyberspace as an additional domain of confrontation, where states conduct espionage, sabotage, and disinformation campaigns against one another (Valeriano & Maness, 2015; Chapple & Seidl, 2021). Existing research on state behaviour in cyberspace identifies several explanatory factors, including strategic rivalry, revisionist ambitions, and political regime type (Valeriano & Maness, 2015; Ebert & Maurer, 2013; Rosenberger, 2020).

An influential selectorate theory and the logic of political survival (Bueno de Mesquita et al., 2003) predict that the size of a leader's winning coalition shapes foreign policy choices, including the decision to initiate conflict. This prediction has been empirically tested and supported in the context of conventional (kinetic) military conflicts (Peceny & Butler, 2004; Weeks, 2014; Adamson, 2020). However, the applicability of the selectorate theory to foreign cyber aggression has not been tested.

The selectorate theory offers divergent views on how the selectorate and winning coalition sizes may affect the state’s behaviour in cyberspace. On the one hand, if the selectorate and winning coalition size effect is similar to the effect on kinetic conflicts, we expect more unprovoked aggression from narrow-coalition

regimes, while broad-coalition regimes should demonstrate mainly restrained or defensive behaviour. On the other hand, because the nature of the cyber domain allows leaders to avoid accountability, we might expect broad-coalition regimes to conduct unprovoked cyber aggression just as likely as narrow-coalition regimes.

Therefore, the analytical question of this research is: "How does the size of the state's winning coalition affect its behaviour in cyberspace?" Specifically, I examine whether the size of the winning coalition predicts the frequency of conducting unprovoked state-backed cyber operations (H1) and the frequency of being targeted by them (H2).

The research design of my study is confirmatory. The selectorate theory allows testable, falsifiable predictions about the relationship between selectorate/winning coalition size and the state's cyber aggression. The Dyadic Cyber Incident and Campaign Dataset (DCID v. 2.0; Maness et al., 2022) recorded state-backed cyber operations in a dyadic format over 20 years. It enables me to perform quantitative hypothesis testing. Because the selectorate theory is well established in the study of kinetic conflicts, extending its predictions to a new domain is a natural confirmatory design choice. The limitation of the quantitative method is that it shifts the focus from the underlying mechanisms of the relationship between regime type and cyber aggression. The confirmatory design allows studying overall trends and predictions, but limits causal inference. Therefore, a plausible causal interpretation of the observed associations is inferred from the theoretical framework.

### *Thesis structure*

The thesis is structured as follows. The literature review surveys the foundational schools of thought in international relations on state aggression, then narrows the discussion to explanations of state behaviour in cyberspace, and identifies the gap of selectorate theory in the cyber domain. The analytical framework conceptualises the key variables and derives three testable hypotheses from the theory. The methodological research design describes the construction of a directed dyad-year dataset, the operationalisation of variables, and the choice of regression models (Negative Binomial and Zero-Inflated Negative Binomial). The results section presents findings across three dataset panels with progressively stricter controls for material capability and kinetic conflict. The discussion situates the findings within the academic debate on regime type and foreign cyber aggression. The following section proposes changes to the national cyber defence strategies. Finally, in the conclusions, I summarise the main research findings, address limitations, and outline directions for future research.

## LITERATURE REVIEW

I conduct this literature review in the following manner. I start with an overview of the foundational schools of thought in international relations regarding state aggression. It sets the stage for the broader academic discussion of the reasons for states' bellicose behaviour towards one another. Then I narrow this discussion down to the application of these international relations theories to the cyber domain. Specifically, I review the academic discussion explaining the factors behind aggressive behaviour in cyberspace. I found that the political regime type is often an indicator of the likelihood that leaders will initiate a conflict, especially within selectorate theory. I proceed to the identification of the literature gap and the construction of the research puzzle and research question. I then conclude the literature review by highlighting the social significance of my research.

### *Major paradigms in international relations theory*

Why do some countries behave more aggressively than others? The prevailing schools of thought on international relationships explain this as follows. Classical realism argues that the aggressive behaviour of states is rooted in human nature, in the "will to power" (Morgenthau, 1948). In this view, states behave aggressively because the individuals who lead them are inherently driven to pursue power and dominate others, resulting in an endless struggle for prestige and security.

Unlike classical realism, neorealism shifts the focus to the anarchic structure of the international order. The absence of a global authority forces states into a "self-help" system (Waltz, 1979; Quinn & Gibson, 2017). Specifically, defensive realism posits that states are power-limited and seek only enough security to maintain the status quo (Waltz, 1979; Walt, 1990). In contrast, offensive realism posits that countries aggressively seek hegemony to ensure their own survival because they can never be certain of others' intentions (Mearsheimer, 2001). Additionally, the rise and fall of dominant powers create cycles of war and change as states attempt to redefine the system to suit their own interests (Gilpin, 1981).

Neoliberal thinkers shift focus to how cooperation persists despite the presence of anarchy (Baldwin, 1993). A key idea of neoliberalism is that international institutions reduce discord by facilitating communication and enabling cooperation (Keohane, 2005). Another important idea is complex interdependence, which posits that as states are increasingly linked through economic and social ties, military aggression becomes more costly and less frequent (Keohane & Nye, 1973; Nye, 1992). However, this "neoliberal order" may now be in decline as a dominant political force in the West (Gerstle, 2018). Therefore, according to neoliberalism, the existence or absence of international institutions, cooperation and trade is a key factor in the state's tendency to be aggressive towards other states.

Constructivism challenges both realism and neoliberalism by arguing that state

interests are not fixed, but rather "constructed" through social interaction. As Wendt (1992, 1999) famously stated, "anarchy is what states make of it." Society and norms redefine what states consider their national interests (Finnemore, 1996), and rules and speech create the very structures of the world in which we live (Onuf, 1998). Ultimately, the way states organise themselves is determined by shared cognitive maps rather than just material power (Ruggie, 1998). Therefore, foreign aggression is a consequence of how states perceive one another (as enemies, rivals, or friends).

### *Cyberspace within international relations*

With the evolution of the Internet, the foundational schools of thought in international relations extend to the study of cyberwarfare (for example, Chapple & Seidl, 2021; Green, 2015; Mueller, 2010; Whyte & Mazanec, 2023). The Internet has evolved from a space of open information exchange to a new area of geopolitical confrontation. Countries use cyberspace to conduct various operations against one another, including strategic espionage, financial theft, disinformation campaigns, sabotage, and attacks on critical infrastructure. The Internet's underlying telecommunications, computing, and storage systems themselves have become core components of a state's critical infrastructure. In the following paragraphs I review an academic discussion regarding state aggression in cyberspace.

One view is that the most engaged countries in cyber conflict are existing geopolitical rivals (Valeriano & Maness, 2015; Dong et al., 2025). In other words, state-sponsored cyber warfare is driven by traditional international power politics. This theory is broadly consistent with a neorealistic view. For countries already at war, cyberspace is merely an additional domain in the battle.

Another view rooted in realism and focuses on revisionist state behaviour (Schweller, 1994). China and Russia are considered the main rising revisionist states that challenge the US's world hegemony (Barrinha & Renard, 2020; Ebert & Maurer, 2013). They might not be able to sustain a full-scale war, but cyber operations enable them to challenge the US while avoiding conventional warfare. In contrast, the literature suggests that other major emerging powers, such as India and Brazil, have adopted less aggressive cyber policies. The explanation for this divergence has been attributed to their democratic regime type (Ebert & Maurer, 2013).

A related view concerns the normative and strategic choice of sub-threshold tools in the conflict. Some scholars suggest treating cyber operations as methods of diplomacy (Barrinha & Renard, 2020) or as a modern form of espionage rather than as a means of war (Valeriano & Maness, 2015). The logic of covert operations in the following. States turn to covert action when they lack legal exemptions from the nonintervention principle, such as a credible self-defence claim or authorisation from an international body. Open violations often have reputational costs, while covert actions allow states to pursue their objectives even while simulating compliance with international norms (Poznansky, 2019). Cyber operations fit this logic particularly well,

as deniability and difficulty in attribution are built-in features of the domain. States that lack the normative standing or legal justification for open aggression may find cyber operations an attractive sub-threshold alternative. Furthermore, most cyber conflicts are intentionally designed to be relatively non-destructive. The primary goal of cyber operations is to demonstrate state capabilities and create a perception of being able to offend, but only at a sub-threshold level. This is explained by the fear that attackers could become part of a major cyberwar, which they would likely lose to the US, a hegemon with superior cyber capacity (Valeriano and Maness, 2015).

Beyond rivalry and strategic choice, a regime type has also emerged as a plausible explanatory factor in the cyber conflict literature. One proposed mechanism is that regime type shapes a state's core ideological view of information exchange on the Internet. Authoritarian regimes that choose to censor and control the Internet tend to adopt more aggressive cyber policies, while interdependent countries that share the ideas of free, borderless information exchange tend to cooperate and primarily defend themselves (Ebert & Maurer, 2013; Rosenberger, 2020). These different approaches to cyberspace governance themselves become a source of rivalry between countries.

The democratic peace theory extends this logic further. While there is much debate about its underlying mechanisms (Doyle, 2005; Rosato, 2003), even critics acknowledge that democratic regimes are less likely to engage in conflict with one another. Existing studies of cyber behaviour similarly acknowledge that autocracies contest democracies or exhibit aggressive behaviour, while democracies tend not to be so aggressive (Barrinha & Renard, 2020; Rosenberger, 2020; Valeriano & Maness, 2015). Hunter et al. (2022) present a quantitative study of the relationship between regime type and state-sponsored cyber aggression. They test competing hypotheses about whether democracies are less, equally, or more likely to initiate cyberattacks than authoritarian states. Their work establishes that regime type is a relevant variable in the cyber domain, though their categorical democracy/autocracy measure cannot isolate the specific institutional mechanism driving the relationship.

There is a debate whether regime institutions that restrain its open military aggression also extend to covert and sub-threshold operations. Political constraints (like congressional opposition) significantly reduced the initiation of covert operations during the Cold War Smith (2019). However, cyber operations may function differently. Democratic leaders can use cyberattacks to satisfy domestic audiences' expectations of forceful action, while avoiding the costs of conventional military engagement (Shandler, 2025). Whether a country's institutional constraints extend to the cyber domain can be also explained by the selectorate theory (Bueno de Mesquita et al., 2003).

### *Application of selectorate theory to the state aggression*

The selectorate theory, or the logic of political survival (Bueno de Mesquita et al., 2003), offers a rational explanation for why some states are more aggressive than others. The theory posits that leaders' primary goal is to retain power, and the strategies they pursue to do so depend on the selectorate (those who have a nominal role in choosing leaders) and the winning coalition (the subset whose support is essential for the leader to remain in office). When the winning coalition is large, leaders must provide public goods, including national security. When the winning coalition is small, leaders sustain loyalty by distributing private goods to a narrow circle of supporters (Bueno de Mesquita et al., 2003). This theory generated a prediction for the state's foreign policy. The narrow-coalition regimes face little domestic political cost for risky or failed aggression. In contrast, broad-coalition regimes face removal from office if aggression fails to serve the broader public interest.

This theory prediction has been empirically tested and confirmed in the context of conventional military conflicts. The study shows that single-party regimes, which have the largest winning coalitions among autocracies, are significantly less likely to initiate militarised interstate disputes. In contrast, personalist regimes, which have the smallest winning coalitions, are both more likely to initiate and to be targeted by disputes. This pattern is related to the coalition size rather than the simple democracy/autocracy binary classification (Peceny & Butler, 2004). The authors examine the conflict behaviour of authoritarian regimes using Geddes' (1999) typology as a proxy for the winning coalition.

Further research finds that personalist regimes and military juntas are more aggressive than civilian single-party regimes, which behave similarly to democracies. However, the coalition size alone is insufficient to explain variation among autocracies (Weeks, 2014). The preferences of the elites who constrain the leader should also be taken into account. A military junta regime may have a small coalition, but that coalition consists of officers who view force as a legitimate instrument of policy. A civilian single-party regime also constrains its leader, but through elites who are more likely to view war as costly and disruptive (Weeks, 2014). This finding suggests that within-autocracy variation requires attention to both the size and composition of the winning coalition.

The selectorate theory’s explanation of the relationship between regime type and its foreign aggression was also supported in a radically different context of ancient Rome. Adamson (2020) finds that the Roman Republic, which had a larger governing coalition than the Empire, fought more battles overall. However, those battles were more oriented toward public goods such as defence. The Empire, with its smaller coalition, fought less frequently but more for private gains such as plunder. Importantly, the effect of coalition size on overall violence is related to the cost of conflict, including demographic and technological factors (Adamson, 2020). The cyber domain represents precisely such a technological shift. Cyber operations are inherently

low-cost, covert, and difficult to attribute (Tsagourias, 2012; Hunter et al., 2022), which might change the audience cost that the selectorate theory mechanism relies upon.

### *Literature gap*

To summarise, current research on states' aggression in the cyber domain varies, including rising revisionism, evolving diplomatic methods, political regime types, and rivalry. Therefore, a state's behaviour in cyberspace is viewed as part of the broader domains of international relations, politics, and conflict studies. However, the applicability of leading theories of state behaviour in conventional (kinetic) conflicts has yet to be tested in cyberspace. In particular, the logic of political survival, grounded in selectorate theory, predicts the initiation of conventional conflicts. According to it, the size of the selectorate and the winning coalition are plausible indicators of the unprovoked state's aggression. However, it has not been tested regarding state aggression in cyberspace.

### *Research puzzle*

The selectorate theory offers different views on how the winning coalition size may affect the state's behaviour in cyberspace. On the one hand, if the winning coalition size effect is similar to the effect on kinetic conflicts, we expect more unprovoked aggression from narrow-coalition regimes, while broad-coalition regimes should demonstrate mainly restrained or defensive behaviour. On the other hand, because the nature of the cyber domain allows leaders to avoid accountability, we might expect broad-coalition regimes to conduct unprovoked cyber aggression just as likely as narrow-coalition regimes.

### *Research question*

How does the size of the state's winning coalition affect its behaviour in cyberspace?

### *Social significance of the research*

Cybersecurity is a public good provided by governments. Many public services and infrastructure used by citizens depend on the state's capability to provide cybersecurity. This idea is reflected in the cyber strategies of the US, UK, EU, and Ukraine. The United Kingdom's Government Cyber Security Strategy aims to ensure that the "core government functions - from the delivery of public services to the operation of National Security apparatus - are resilient to cyberattack" (HM Government, 2022, p. 8). The United States frames its cyber strategy as the defence of the safety, security, and prosperity of the American people (The White House, 2026). The European Union seeks to "build resilience to cyber threats and to ensure that citizens and businesses benefit from trustworthy digital technologies" (European

Commission & High Representative, 2020). Ukraine's strategy likewise aims to "ensure their socio-economic development in the digital world, which requires acquiring the ability to effectively deter destructive actions in cyberspace" (Президент України, 2021).

Providing cybersecurity as a public good means defending a state from actors like cybercriminal groups or other states. "The threat from nation state actors is of considerable concern, with nearly half of nation state activity being targeted at governments across the world" (HM Government, 2022, p. 17). The United Kingdom, being among the most-targeted states in cyberspace, defends from previously observed cyber threats (HM Government, 2022). Ukraine defends itself against Russia (Президент України, 2021) because Russia has been its obvious aggressor in both the kinetic and cyberspace domains for many years. The European Union names no adversary in its strategy, but has imposed sanctions targeting the Russian government after recognising that it sponsors cyberattacks (European Commission & High Representative, 2020; Council of the EU, 2024). The United States goes beyond exclusively defensive strategy, committing to detect and defeat cyber adversaries before they breach its networks (The White House, 2026, p. 4). Therefore, governments usually predict the likely sources of cyber aggression reactively, based on recent experience. And their cyber strategies reflect those predictions.

Therefore, this research is socially significant for cybersecurity strategy policy-making. This study aims to improve national cybersecurity strategies by predicting state-sponsored cyber aggression using the selectorate theory. Currently, policymakers primarily prepare to defend against former aggressors and the current enemy in the ongoing kinetic conflict. And this is a fair approach. However, the value of this study lies in improving current strategy by modelling which other states are likely to be aggressors and against whom. For example, to model which states Ukraine is not at war with, but pose it a threat in cyberspace.

## ANALYTICAL FRAMEWORK

### *Conceptualization*

The dependent variable in my research is state-backed cyber operations. I do not account for cyber-activity by criminals or other non-state-affiliated groups because their motives differ from those of the regime. While the terms "cyber operations," "cyber attacks," "cyber incidents," and "cyber conflicts" are often used interchangeably, I find "cyber operations" to be a more precise term. To conceptualise my dependent variable, I borrow the following definition by Valeriano & Maness (2015, p. 21): "the use of computational technologies for malevolent and destructive purposes in order to impact, change, or modify diplomatic and military interactions between states." Such a definition emphasises actors' motives and their foreign policy choices. The specific methods used in such cyber operations vary and evolve with time. According to the

available data, the most common methods include network intrusion, inflation, DDoS attacks, and website defacements.

The independent variable in my research is the size of the state winning coalition, which represents the political regime structure. A winning coalition is a central concept in selectorate theory (Bueno de Mesquita et al., 2003). Therefore I use the conceptualization provided by Bueno de Mesquita & Smith (2021, p.2): "The selectorate is the set or proportion of residents in a polity who have at least a nominal say in choosing leaders and W [winning coalition] is the minimal subset or proportion of S whose support is essential for an incumbent to retain power or for a challenger to come to power." Therefore, I assume that the winning coalition is a plausible indicator of the state political regime structure, even though some autocracies might have much wider winning coalitions than others (for example, authoritarian corporate vs neopatrimonial regimes).

### *Theoretical framework*

My theoretical framework is based on the selectorate theory and the logic of political survival (Bueno de Mesquita et al., 2003). Instead of categorising regimes as democracies or autocracies, the selectorate theory examines the internal power dynamics of each state through two groups: the selectorate (those who are choosing leaders) and the winning coalition (the subset whose support is essential for the regime to survive). The theory posits that leaders' primary goal is to retain power, and the strategies they pursue depend on the relative size of these two groups.

The expected relationship between the size of the winning coalition and foreign aggression follows from the theory's core mechanism. When the winning coalition is large, leaders must provide public goods, such as national security and economic welfare. Private rewards in such a case are inefficient because they would be spread too thinly across a broad selectorate or coalition. Failed or costly aggression (such as unprovoked non-justified cyber operations) diverts resources from public goods provision and risks the leader's removal from office. When the winning coalition is small, leaders sustain loyalty by distributing private goods to a narrow circle. Their allegiance holds regardless of policy performance. The domestic political cost of risky or failed aggression is therefore small for narrow-coalition leaders (Bueno de Mesquita et al., 2003).

This mechanism has been supported for conventional military conflict by the research of Peceny and Butler (2004). They show that single-party regimes (the largest winning coalitions among autocracies) are significantly less likely to initiate militarised interstate disputes. In contrast, personalist regimes (the smallest winning coalitions) are more likely to initiate and to be targeted. Weeks (2014) corroborates this pattern with an independent regime typology. Furthermore, Adamson (2020) finds support for this mechanism in the context of ancient Rome. Bueno de Mesquita et al. (2003)

further specify that broad-coalition leaders are not entirely passive. They do initiate conflicts when victory is likely to be swift, and costs are low.

I test whether this relationship extends to the cyber domain. The expected direction of the effect is as follows. Narrow-coalition regimes, where leaders face minimal domestic accountability for foreign policy failure, should conduct more unprovoked cyber operations. Broad-coalition regimes, where leaders risk removal for costly or unjustified aggression, should conduct fewer of them. This translates to the first hypothesis, H1: the larger the winning coalition, the lower the frequency of conducting unprovoked state-backed cyber operations.

The selectorate theory also predicts which states make attractive targets. Broad-coalition regimes mobilise resources more effectively and fight harder when attacked, making them dangerous opponents that others should avoid provoking. Narrow-coalition regimes, by contrast, underinvest in public goods, including national defence, making them weaker and more attractive targets (Bueno de Mesquita et al., 2003; Peceny & Butler, 2004). If this logic extends to cyberspace, narrow-coalition states should be targeted more frequently. This translates to the second hypothesis, H2: the smaller the regime's winning coalition, the more frequently it is targeted by unprovoked cyber operations.

Therefore, my research design is confirmatory, e.g. hypothesis testing. I analyse whether the size of a winning coalition influences its regime's behaviour in cyberspace. Specifically, I focus on state-backed cyber operations towards other states.

### *Hypothesis*

**H0:** Winning coalition does not affect unprovoked state-backed cyber operations.

**H1:** The larger the regime's winning coalition, the less frequently it conducts unprovoked cyber operations.

**H2:** The smaller the regime's winning coalition, the more frequently it is targeted by unprovoked cyber operations.

## METHODOLOGICAL RESEARCH DESIGN

The study's design is quantitative. This choice is driven by the confirmatory nature of my research. I aim to confirm the applicability of selectorate theory to the dataset of state-initiated cyber operations. For dataset processing (cleaning and merging), I use RStudio. It is a free IDE for the R programming language, designed for data science, statistics, and analysis. The primary scripts are data_preparation.R and models.R. The generated panel data, the relevant R code and visualisations are available in the GitHub project, which is referenced in the Appendices section. The GitHub project structure is described in detail in the README.md file, which is also referenced in the Appendices section.

### *Independent variable operationalisation*

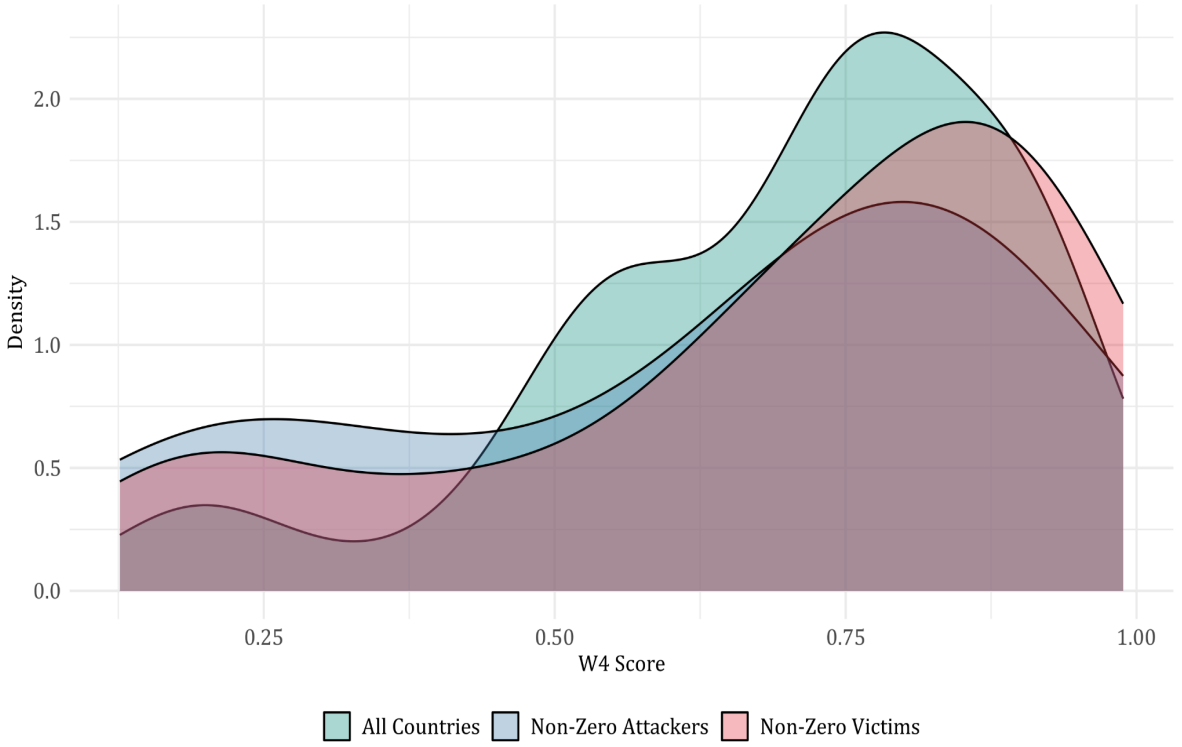
The empirical testing of selectorate theory has long been criticized by the lack of a convincing measure of winning coalition size. Bueno de Mesquita et al. (2003) themselves acknowledged that their original indicators were "much too crude," and other critics reinforced this concern (Clarke & Stone, 2008; Gallagher & Hanson, 2015). Peceny and Butler (2004) worked around this limitation by using Geddes' categorical regime typology as a proxy.

Bueno de Mesquita and Smith (2021) resolved the measurement problem by developing a new continuous indicator of coalition size (notated W4) based on institutional variables from the V-Dem project (Coppedge et al., 2021). It directly addresses longstanding critiques of earlier winning coalition operationalisations (Bueno de Mesquita & Smith, 2021, p. 3) by replacing the original five-category ordinal measure with an index spanning thousands of unique values (Bueno de Mesquita & Smith, 2021, p. 9). In comparisons with eight widely used regime-type indicators across 30 dependent variables, a new winning coalition index outperforms all alternatives (Bueno de Mesquita & Smith, 2021, p. 1).

This newest measurement, containing the winning coalition indexes for countries up to 2020, is published by Smith (2022) in the Harvard Dataverse. Therefore, this dataset is the best available option for measuring the size of the winning coalition. A unit of observation in the published dataset, the winning coalition index, is ranging from 0 to 1 for a specific year and country. In my work, I use this index without additional transformations. Therefore, the winning coalition index (W4) becomes my measure for the independent variable.

Panel data A (see “Data preparation for processing” subsection and Table 3 for details) covers 174 countries observed in 2007–2020. The W4 index ranges from 0.13 to 0.99 in the sample (mean = 0.70, median = 0.74, sd = 0.20) for this timeframe. Most countries have a moderately high W4, but many also have narrow coalitions, so the W4 index is left-skewed (skewness ≈ -0.98). Graph 1, built in R using the ggplot2 package, compares this overall distribution with the subsets of countries that conducted at least one cyber operation as an attacker (16 countries) and that were targeted at least once as a victim (30 countries). The attacker subset has a noticeably lower mean (0.63) and a wider spread, with extra density in the low-W4 range. The victim subset, by contrast, has a mean of 0.69 (almost the same as the all-country mean of 0.70), with no clear skew toward higher W4.

**Graph 1. Distribution of country-level means of Winning Coalition Index.**




Notes: 174 countries, 2007–2020 (Panel A). "Non-zero attackers" are countries that conducted at least one cyber operation in the panel. "Non-zero victims" are countries that are countries targeted at least once. Source: own calculations based on Smith (2022). Built in R using the ggplot2 package.

***Dependent variable operationalisation***

To measure state-backed cyber operations, I utilise the Dyadic Cyber Incident and Campaign Data (DCID) v. 2.0, developed by Maness et al. (2022). The unit of observation in this dataset is a unique cyber operation between two rival countries. The dataset contains records of cyber operations from 2000 to 2020. One operation may encompass thousands of events and span years, or it may be a single one-day incident. Additionally, each observation includes information on timing, as well as categorical data on severity, methods, objectives, and other related details.

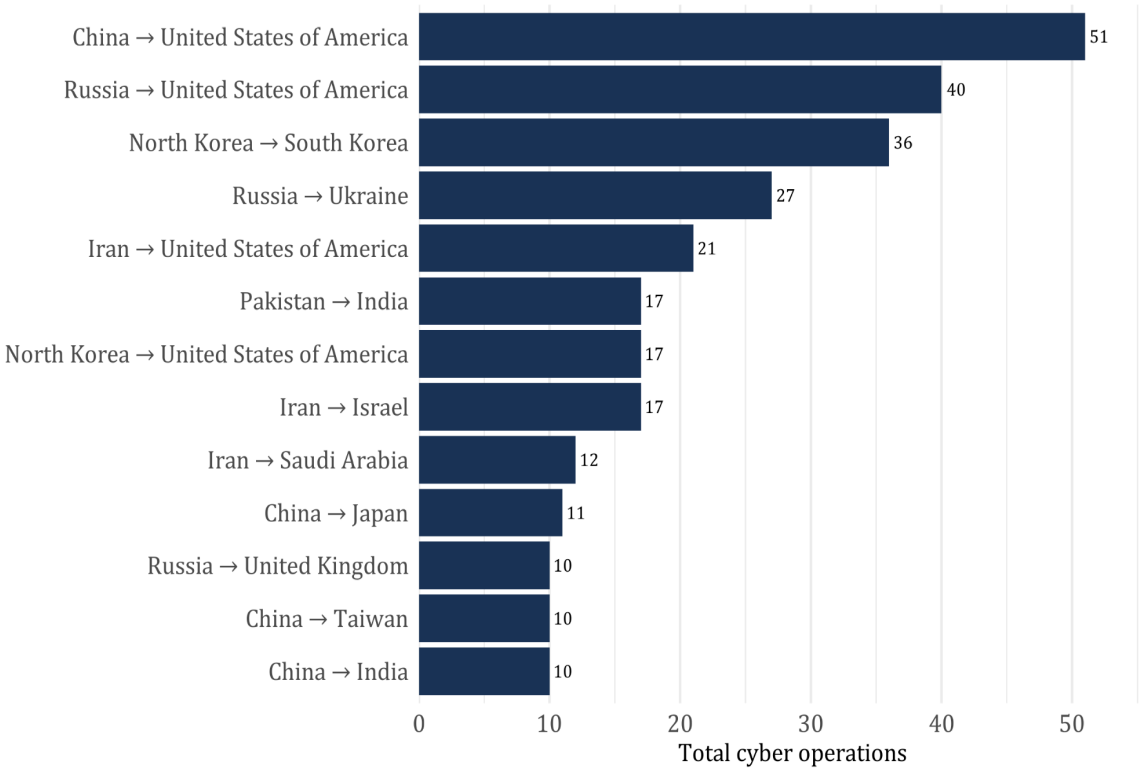
The dataset contains observations only about international cyber operations of nation-states. The attacks by cybercriminals and other non-state actors are not recorded. Such filtering makes the DCID dataset a better choice than alternatives, such as reports from antivirus or Endpoint Protection Platform companies, which typically include operations by non-state actors.

I aggregate the data from the DCID, add non-listed countries, and include all observed years, essentially creating a panel data set (see the sub-section “Data preparation for processing” for more details). As a result, I operationalise the dependent variable as a count of cyber operations by attacker to victim in a specific

year. Therefore, this incident count (the measure of the dependent variable) in my regression-ready dataset is a non-negative integer.

Panel A (see Table 3 for details) covers the years 2007–2020 and contains 398 cyber incidents produced by 16 attacker states against 30 victim states. The distribution across pairs is highly concentrated. Graph 2, built in R using the ggplot2 package, shows the twelve most active attacker-victim dyads. The four most active pairs alone account for 154 incidents, almost 40% of the total.

**Graph 2. Most active attacker-victim pairs.**




Notes: 12 most active directed dyads in Panel A, 2007–2020. Source: own calculations based on data from Maness et al. (2022). Built in R using the ggplot2 package.

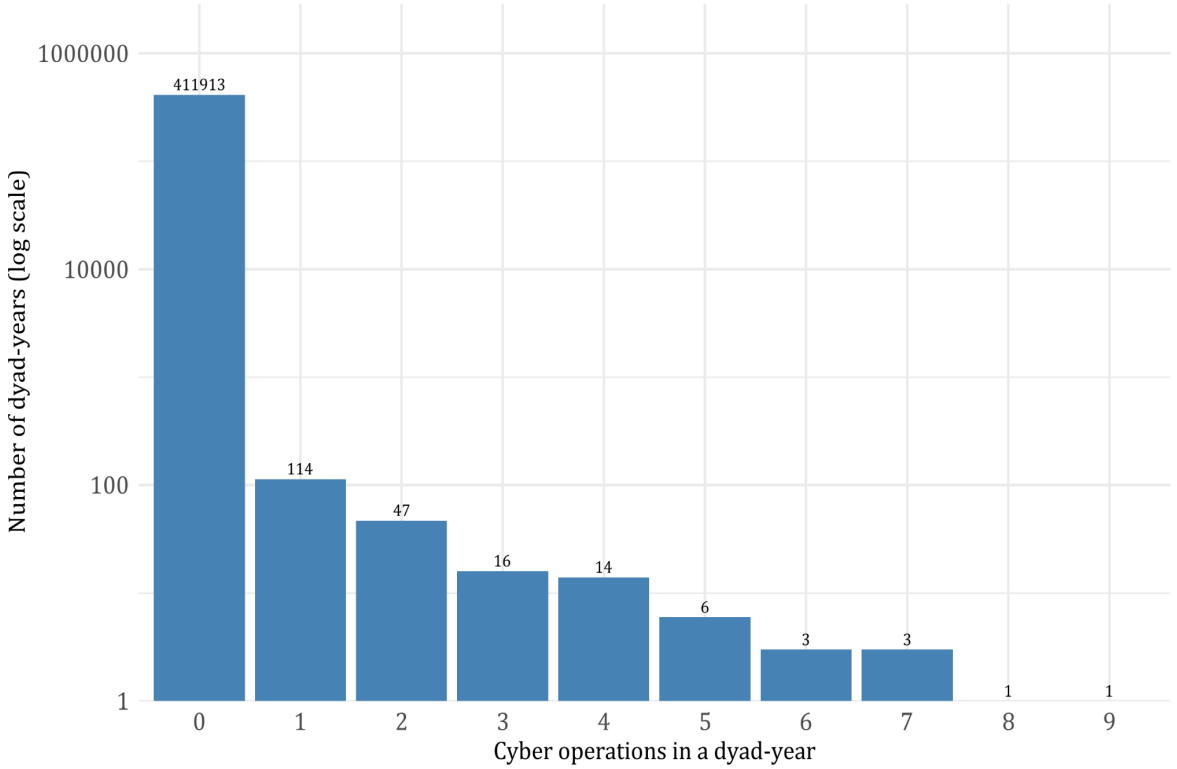
***Methods***

To test my hypothesis, I choose Negative Binomial (NB) and Zero-Inflated Negative Binomial (ZINB) regression methods. The rationale for this choice is as follows. First, the data is heavily overdispersed. The variance of Incident_Count is approximately three times its mean, and a likelihood ratio test of Poisson against Negative Binomial (LR = 1801.5, $p < 0.001$, reported in descriptive_statistics.R) decisively rejects the Poisson model choice. All count-only models, therefore, use the Negative Binomial estimator.

Second, the data are heavily zero-inflated. More than 99% of dyad-years across all three panels contain no cyber operations (see the sub-section “Data preparation for processing” for more details). Many of these zeros are structural (directed dyads that

essentially never produce cyber operations) because the attacker lacks the capability, because the victim is not a viable target, or because the dyad pair has no conflictual relationship. These structural zeros are distinct from observations for dyads that are plausibly active but lack recorded incidents in a given year (due to information gaps). The Zero-Inflated Negative Binomial addresses this difference by jointly estimating an inflation equation that predicts whether a dyad-year is a structural zero and a count equation that models the frequency of operations among the remaining dyad-years (see the section "Hypothesis testing" for more details).

**Graph 3. Dyad-year count distribution.**




Notes: number of directed dyad-years by incident count in Panel A (2007–2020). 99.95% of directed dyad-years record zero operations, which justifies the choice of ZINB regression. Source: own calculations based on data from Maness et al. (2022). Built in R using the ggplot2 package.

Third, panel data of this type have temporal dependence. Year fixed effects are therefore included in every model in this analysis. M7, the primary model, applies year fixed effects to both the count and inflation stages. See the "ZINB model with year fixed effects in both stages (M7, primary model)" sub-section for more details.

### *Hypothesis testing*

To test the hypothesis, I use seven main models (M1-M7) and six robustness models (R1–R6). The specifications of the main models are summarised in Table 4 in

the Results section. The specifications of the robustness models, as well as the model results, are provided in Tables 6, 7, and 8 in the Appendices section. In this section, I provide the formulas and detailed descriptions of the methods used in the main regression models.

Each NB and ZINB specification estimates both the victim_W4 coefficient ($\beta_2$) and the attacker_W4 coefficient ($\beta_1$). Therefore, the same models test both H1 and H2.

*NB models with year fixed effects (M1, M2, M4, M5)*

The dependent variable is the count of cyber operations conducted by attacker *i* against victim *j* in a year *t*, denoted $Y_{ijt.}$ It is marked as Incident_Count in M1, M2, and M4, and as Incident_Count_Clean in M5. The variable name contains "_Clean" because it reflects additional filtering of defensive and kinetic-conflict-related operations. $Y_{ijt.}$ It is regressed on the attacker's winning coalition index (attacker_W4) and the victim's winning coalition index (victim_W4). I include the victim_W4 to control for the possibility that states with specific coalition sizes are systematically more likely to be targeted, which could otherwise confound the estimated effect of attacker_W4.

Control variables differ by model, depending on data availability across dataset panels (see Table 3). All four specifications (M1, M2, M4, M5) include GDP per capita (The World Bank, n.d.; Taiwan Directorate-General of Budget, n.d.; Bank of Korea, n.d.). M2, M4, and M5 also add control of the Composite Index of National Capability, CINC (Greig & Enterline, 2021). And M4 additionally includes control for Militarized Interstate Disputes, MID (Maoz et al., 2021) for the use of force at hostility level > 3. To address the temporal dependence inherent in panel data, all models include year fixed effects that absorb shocks common to all directed dyads in a given year.

Therefore, negative binomial specification with year fixed effects for M1, M2, M4, and M5 takes the form:

$$\log (E [Y_{ijt}] ) = \beta_1(\text{attacker\_W4}_{it}) + \beta_2(\text{victim\_W4}_{jt}) + \gamma' Z_{ijt} + \delta_t ,$$

where:

- $Y_{ijt}$ is the count of cyber operations by attacker *i* on victim *j* in year *t* (dependent variable).
- $\beta_1$ (attacker_W4$_{it}$) is the effect of the attacker's (*i*) winning coalition index (attacker_W4) on the expected count of cyber operations in year *t,* holding everything else constant.
- $\beta_2$(victim_W4$_{jt}$) is the effect of the victim's (*j*) winning coalition index (victim_W4) on the expected count of cyber operations in year *t*, holding all other variables constant.

In other words, *exp*($\beta_1$)-1 shows the percentage change in the expected count from a one-unit increase in attacker_W4, holding everything else constant. The *exp*($\beta_2$)-1

shows the percentage change in the expected count from a one-unit increase in victim_W4, holding everything else constant.

- $Z_{ijt}$ is the vector of control variables (which differ by model, as described above). And $\gamma$ is the vector of coefficients on those controls. It means that each element of $\gamma$ is the coefficient on the corresponding variable in $Z_{ijt}$. For example, in M2 $\gamma'Z_{ijt}$ expands to $\gamma_1(\text{attacker\_CINC}_{it}) + \gamma_2(\text{victim\_CINC}_{jt}) + \gamma_3(\text{attacker\_ln\_GDP}_{it}) + \gamma_4(\text{victim\_ln\_GDP}_{it})$.
- $\delta_t$ is the year fixed effect in year *t*. Standard errors are clustered at the directed dyad level to account for within-dyad correlations across years.

Hypothesis H1 is supported if $\beta_1 < 0$ and is statistically significant. A larger attacker's winning coalition is associated with a lower expected count of cyber operations initiated by a state.

Hypothesis H2 is supported if $\beta_2 < 0$ and is statistically significant. A larger victim's winning coalition is associated with a lower expected count of cyber operations targeting that state.

*ZINB models with year fixed effects in the count stage (M3, M6)*

The zero-inflated negative binomial (ZINB) is designed for data with many zeros, just like my regression-ready dataset panels. The majority of directed dyad-years contain no operations at all, and one of the reasons is that many state pairs are structurally incapable of conducting them.

The ZINB decomposes the model outcome into two distinct processes (stages). The inflation stage is a logit model of whether a dyad-year belongs to a structural zero category. It means a dyad-year in which an attacker state lacks the capability to conduct a cyber operation against a victim state, regardless of motivation. To be clear, a structural zero is a property of the pair "attacker→victim" in a given year, not the attacker property alone. A dyad can be a structural zero observation because the attacker lacks the capability to conduct cyber operations, because the victim is not a viable target (nothing to attack), because the two states have no conflictual relationship that would motivate an operation, or any combination of those. In other words, the inflation stage separates pairings that essentially never produce operations from pairings that are active.

The count stage is a negative binomial count process modelling the remaining, non-structural zero dyad-years. It means directed dyad-years in which a cyber operation is structurally possible, whether it actually occurred (was it recorded in a given year or not). In other words, the count stage models the frequency of attacking only when a state is capable of doing so, thereby capturing the attacker's choice. Year fixed effects are included in the count stage to control for temporal dependence.

The dependent variable $Y_{ijt}$ is Incident_Count for M3 and Incident_Count_Clean for M6. As in the NB models, the count stage regresses $Y_{ijt}$ on the attacker's winning

coalition index (attacker_W4) and the victim's winning coalition index (victim_W4) with the same controls as M2 (attacker and victim CINC, attacker and victim GDP per capita). The inflation stage also includes attacker and victim CINC, because it represents the proxy for whether a specific attacker state has the capability to conduct a cyber operation against a specific victim state in a given year. To be precise, the inflation stage does not identify attacker capability as such. Instead, it identifies whether the directed dyad is a plausible "attacker→victim" pairing.

Therefore, ZINB specification for M3 and M6 takes the form:

(1) of ZINB non-structural-zero part (count stage):

$$\log\left(E\left[Y_{ijt} \mid S_{ijt} = 0\right]\right) = \beta_1(\text{attacker\_W4}_{it}) + \beta_2(\text{victim\_W4}_{jt}) + \gamma' Z_{ijt} + \delta_t,$$

where:

- $S_{ijt}$ is an indicator that equals 1 if a dyad-year ($i$, $j$, $t$) is a structural zero and 0 otherwise.
- All other variables in the count stage ($\beta_1$, $\beta_2$, $\gamma' Z_{ijt}$, and $\delta_t$) are defined as in the NB specification above.

(2) of ZINB structural zero part (inflation stage):

$$\text{logit}\left(P\left(S_{ijt} = 0\right)\right) = \alpha_0 + \alpha_1(\text{attacker\_CINC}_{it}) + \alpha_2(\text{victim\_CINC}_{jt}),$$

where:

- $\alpha_0$ is the inflation-stage intercept, representing the probability that a directed dyad belongs to the structural-zero class before accounting for the capability of either state.
- $\alpha_1$ and $\alpha_2$ are the effects of attacker and victim capability (CINC) on the probability of being a structural zero.
- $S_{ijt}$ is defined as above in the count stage.

Hypotheses are tested on the count-stage coefficients. H1 is supported if $\beta_1 < 0$ and statistically significant in the count stage. Among dyads in which attackers have the capability to conduct cyber operations against victims, a larger attacker winning coalition is associated with a lower expected count of cyber operations initiated by a state.

Hypothesis H2 is supported if $\beta_2 < 0$ and statistically significant in the count stage. Among dyads where attackers have the capability to conduct cyber operations against victims, a larger victim winning coalition is associated with a lower expected count of cyber operations targeting that victim.

*ZINB model with year fixed effects in both stages (M7, primary model)*

The primary specification, M7, extends M6 by applying year-fixed effects to both the count and inflation stages of the ZINB. It provides more controls for temporal dependence. M7 also uses the methodologically cleanest dependent variable, Incident_Count_Clean, from panel C. Together, they make M7 the strongest test of H1 and H2 on the available data.

Therefore, M7 ZINB specification takes the form:

(1) of ZINB non-structural-zero part (count stage):

$$\log (E [Y_{ijt} | S_{ijt} = 0] ) = \beta_1(\text{attacker\_W4}_{it}) + \beta_2(\text{victim\_W4}_{jt}) + \gamma' Z_{ijt} + \delta_t,$$

where all the variables are the same as in the M6 count stage (this formula is identical).

(2) of ZINB structural zero part (inflation stage):

$$\text{logit} ( P (S_{ijt} = 0) ) = \alpha_1(\text{attacker\_CINC}_{it}) + \alpha_2(\text{victim\_CINC}_{jt}) + \eta_t,$$

where:

- $\eta_t$ is the year fixed effect in the inflation stage, absorbing temporal variation in the structural-zero dyad-years and replacing a separately estimated in M6 inflation-stage intercept $\alpha_0$.
- All other terms are defined as in the M3 and in the M6 inflation stage specification.

The explicit difference between the $\delta_t$ and the $\eta_t$ is related to the capability threshold. The inflation stage fixed effects $\eta_t$ control for year-by-year temporal effects in global cyber capability. For example, due to global technological development, in 2007 the baseline probability that any regime would have cyber capabilities was much lower than in 2020. The count stage fixed effect $\delta_t$ controls for year-by-year temporal effects that might drive the frequency of attacks among states that are already capable. For example, if global political motivations change in a given year due to major crises, already technologically capable states might be more active in cyberspace.

As with M3 and M6, for M7 hypotheses are tested on the count-stage coefficients. By controlling for $\eta_t$ in the inflation stage, I made the data passing to the count stage cleaner. Therefore, the count stage can estimate the coefficients for winning coalition variables $\beta_1$ and $\beta_2$ more accurately.

As with M3 and M6, for M7 hypothesis H1 is supported if $\beta_1 < 0$ and statistically significant in the count stage. Among dyads where attackers have the capability to conduct cyber operations against victims, a larger attacker winning coalition is

associated with a lower expected count of cyber operations initiated by a state.

Hypothesis H2 is supported if $\beta_2 < 0$ and statistically significant in the count stage. Among dyads where attackers have the capability to conduct cyber operations against victims, a larger victim winning coalition is associated with a lower expected count of cyber operations targeting that victim.

### *Data Collection*

I have collected publicly available datasets directly from the source websites. The collected data is summarised in Table 1.

**Table 1. Data sources and their purpose.**

| Data source name | Filename in the source code | Data source URL | Purpose |
|---|---|---|---|
| The Dyadic Cyber Incident and Campaign Data (DCID), version 2.0 | DCID_2.0_Release_update_February_2023.xlsx | https://www.ryanmaness.com/cyber-conflict-dataset | For the dependent variable. |
| Winning Coalition Index (W4) | NewWmeasure.csv | https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/UYLXRO | For the independent variable. |
| COW Country Codes | COW-country-codes.csv | https://correlatesofwar.org/cow-country-codes | For translating country codes in DCID into county names and for mapping countries between different datasets. |
| CINC (NMC) | NMC-60-abridged.csv | https://correlatesofwar.org/data-sets/national-material-capabilities/ | Control variable, Composite Index of National Capability. |
| World Bank, GDP per capita | a14efc5a-7fe8-4ea4-b8ed-57b7727e3394_Data.csv | https://databank.worldbank.org/source/ | Control variable, GDP data for most countries. The World Bank does not |

| | | | |
|---|---|---|---|
| | | world-development-indicators | contain information on North Korea and Taiwan. |
| Bank of Korea (NK). I manually composed this file from yearly reports (2007-2020) | Indicators_NK.xlsx | https://www.bok.or.kr/eng | Gross Domestic Product Estimates for North Korea. |
| Taiwan National Statistics | E018101010_00203 4281.csv | https://nstatdb.dgbas.gov.tw/dgbasall/webMain.aspx?k=engmain | Gross Domestic Product for Taiwan. |
| Militarized Interstate Disputes (MID), Dyadic MID v4.03 | dyadic_mid_4.03.csv | https://correlatesofwar.org/data-sets/mids/ | Control for ongoing kinetic conflict |

Notes: this table summarises the data sources I used to create regression-ready panel data.

### *Data preparation for processing*

All the source code for data preparation, replication and processing, along with regression models, is available in the corresponding GitHub repository (see the Appendices section). In the data_preparation.R script, I process the source data for regression analysis. The detailed explanation of each step can be found in the script's comments, while in this sub-section, I provide a general overview of the process.

#### *Independent and dependent variables preparation for processing*

The original DCID dataset (DCID v. 2.0; Maness et al., 2022) identifies attackers by COW country codes (Correlates of War Project, n.d.) in the “initiator” field. The data preparation script matches this code to the COW country code dataset to obtain the attacker's country name. Then determines the victim by checking whether the attacker corresponds to StateA or StateB in the incident record - the other state in the pair is the victim. It produces observations of directed dyads, where each cyber incident generates one observation with an identified attacker and victim.

The original cyber incidents dataset (DCID v. 2.0; Maness et al., 2022) is a list of separate cyber operations, along with metadata. I aggregate this list so that the unit of observation is a directed (e.g., from one country to another) count of cyber incidents per year for a pair of countries. For example, if China had attacked the US 9 times in 2014, that would be 9 separate observations in the original dataset, but 1 unit of

observation in my processes dataset: "China → US, 9 times in 2014". At the same time, I make a separate observation for the same year, in the reverse direction, for the same two countries. For example, "US → China, 0 times in 2014". See Table 2 for details.

The original dataset (DCID v. 2.0; Maness et al., 2022) contains 429 cyber incidents from 2000 to 2020 and spans across 31 countries only. Therefore, in most of the 174 countries in the resulting regression-ready panels, no cyber incidents are observed. As a result, the processed data becomes largely inflated with zero observations. I handle this by using the Negative Binomial and Zero-Inflated Negative Binomial regressions. These statistical methods are designed to analyse count data with overdispersion and excess zeros.

For each year and each country, I add the winning coalition index (Smith, 2022). As a result, the winning coalition index of the attacker (attacker_W4) and the winning coalition index of the victim (victim_W4) are two columns of the independent variable.

To summarise, I combine data from both the winning coalition dataset (Smith, 2022) and the cyber incident dataset (Maness et al., 2022), and add control variables (listed in Table 1). Finally, I aggregate the directed (e.g., attacker → victim) incidents to count the number of operations for each rivalry dyad pair per year, making it a panel data set. Therefore, the unit of observation in the resulting datasets is the "number of directed state-backed cyber operations in a year". For example, in the observation described in the first row of Table 2, China attacked the US 9 times in 2014.

**Table 2. Example of the resulting observations.**

| Row number | Attacker | Target | Year | Incident Count | Attacker's Winning coalition index | Target's Winning coalition index |
|---|---|---|---|---|---|---|
| 1 | China | US | 2014 | 9 | 0.1642758 | 0.9695077 |
| 2 | North Korea | US | 2017 | 8 | 0.1890847 | 0.9420754 |

Notes: own calculations based on data from the public data sets: "The Dyadic Cyber Incident and Campaign Dataset, version 2.0" (Maness et al., 2022) and "Replication data for: A new indicator of coalition size (Version 1)" (Smith, 2022).

*Control variables preparation for processing*

After incident aggregation, I merge the control variables into my observations. GDP per capita data is available for all observed years for most countries via the World Bank (The World Bank, n.d.). However, it does not include information on North Korea and Taiwan, so I additionally used data from the Bank of Korea (n.d.) and the Taiwan Directorate-General of Budget (n.d.). Also, there is no separate GDP data for Zanzibar, but there are no observed cyberattacks related to Zanzibar, either. So I dropped

Zanzibar from the resulting dataset, assuming it would not be a meaningful observation.

Two additional control variables are the Composite Index of National Capability (CINC; Greig & Enterline, 2021) and Militarised Interstate Disputes (MID; Maoz et al., 2021) by the Correlates of War project. Unfortunately, they are available only up to 2016 and 2014, respectively. To test the hypotheses, I created three regression-ready dataset panels based on data availability: df_model_2020.csv, df_model_2016.csv, and df_model_2014.csv. These are the main outputs of the data_preparation.R script. They are available in the GitHub repository referenced in the Appendices section.

*Temporal filtering*

From 2000 to 2007, there were only 26 observations (about 6% of the total) in the original DCID dataset. I intentionally dropped them to avoid unnecessary overinflation by zeros. So all three dataset panels start from 2007.

The seven models partition into three panel groups. A summary of these panel groups is available in Table 3. Panel A (for M1) is the broadest. It contains data for 2007–2020, with W4 and GDP as controls. CINC is unavailable beyond 2016, so Panel A cannot include capability measures and therefore cannot accommodate the ZINB inflation stage. Therefore, a ZINB regression on Panel A is not tested. Panel B (M2, M3, M4) covers 2007–2016 with full controls (W4 + CINC + GDP); M3 adds the ZINB, and M4 adds a kinetic-conflict control via MID hostility level $\geq 4$ (Maoz et al., 2021).

Panel C (M5, M6, M7) uses Incident_Count_Clean as a measure of the dependent variable. The panel excludes 43 incidents in total: 7 were manually coded as cyber-to-cyber retaliation (see Table 9 in the Appendices section), 36 were linked to active militarised disputes (MID hostility $\geq$ 4), and 4 satisfied both criteria. An additional 122 dyad-years in which the dyad was engaged in kinetic conflict are dropped from the panel entirely, eliminating false zeros. The resulting panel contains 235864 dyad-year observations with 145 unprovoked cyber incidents. M5 is the NB regression on this clean dependent variable. M6 adds ZINB. M7 adds year fixed effects to both ZINB stages and it is the primary model.

**Table 3. Overview of the regression-ready data panels.**

| Dataset Panel | Filename | Control variables | Years covered | Number of cyber incidents | Number of observations (dyad-year incidents) | Non-zero observations |
|---|---|---|---|---|---|---|
| Panel A | df_model_2020.csv | GDP per capita | 2007–2020 | 398 | 412118 | 205 (0.05%) |
| Panel B | df_model_2016.csv | GDP per capita, CINC | 2007–2016 | 258 | 295154 | 136 (0.05%) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | (and MID up to 2014 – only for model M4) | | | | For M4: 101 |
| Panel C | df_model_2014.csv | GDP per capita, CINC, filters using MID and manual filtering out defensive cyber operations | 2007–2014 | 145 | 235864 | 79 (0.03%) |

Notes: creation of these dataset panels is described in the current sub-section "Data preparation for processing", while the content of the data_preparation.R script is available in the GitHub reference in Appendices section. All data sources and variable references are listed in Table 2.

*Filtering out kinetic-related cyber operations*

I noticed that many cyber operations occur during militarised (kinetic) conflicts. For example, Russia attacked Georgia in cyberspace 8 times in 2008 while invading on land. Such observations are theoretically expected. Countries use cyber as a method of war, as documented in existing research (Valeriano & Maness, 2015). Therefore, to control for ongoing kinetic conflict, I use Militarized Interstate Disputes, MID data (Maoz et al., 2021) in two ways. Firstly, in model M4 for dataset Panel B, I add MID (hostility $\geq 4$) as a control variable. And in robustness check R1, I add MID at any hostility level. Second, for the dataset Panel C, I use MID to exclude dyad-years with a MID hostility level of 4 (use of force) or 5 (interstate war), following the COW coding scheme (Maoz et al., 2021). This filter significantly reduces the number of observations in the regression, but allows me to analyse cyber aggression unrelated to kinetic conflicts. It makes Panel C (df_model_2014.csv) the methodologically strongest dataset panel out of three.

To identify specifically *unprovoked* cyber aggression, I manually reviewed the political objective description of each observation in the original DCID dataset for the years 2007-2014. I identified 7 cyber operations that could be classified as "active cyber defence" outside the defended cyber infrastructure (Schmitt, 2017, p. 563) or as a "hack back… action against an identified source of a malicious cyber operation… designed to mitigate the effects of, or stop, the malicious activity, or to gather technical evidence that can be used for attribution purposes." (Schmitt, 2017, p. 565). 4 out of 7 such active cyber defence operations overlapped with intensive kinetic conflicts, while 3 did not. I hardcoded the names of the 7 observations in the script to filter them out of the Panel C dataset, so the dependent variable counts contain only *unprovoked* cyber aggression. The data_preparation.R script additionally produces incidents_excluded.csv and incidents_kept.csv datasets for transparency. The 7 cyber operations that could be

classified as “active cyber defence” are listed in the Table 9 of the Appendices section. The scripts are available in the GitHub repository referenced in the Appendices section.

### *Models*

*Main models overview*

In the models.R script (see GitHub repository referenced in the Appendices section), I load all three dataset panels produced by data_preparation.R to run the regression models. The detailed explanation of each step can be found in the comments within the script. In this section, I provide an overview of the same process. Essentially, I developed seven models (M1–M7) to jointly test H1 and H2, along with a series of robustness checks reported in the Appendices and the supplementary robustness.R script. Table 4 summarises the specifications of the seven main models and their relation to the respective data panels A, B and C.

**Table 4. Model specifications.**

| Model | Estimator | Specification | Purpose |
|---|---|---|---|
| Panel A Dataset (2007–2020) | | | |
| M1 | NB | W4 + GDP + Year FE | H1 & H2 on the broadest panel |
| Panel B Dataset (2007–2016) | | | |
| M2 | NB | W4 + CINC + GDP + Year FE | H1 & H2 with full controls |
| M3 | ZINB | W4 + CINC + GDP + Year FE \| CINC | ZINB on Panel B |
| M4 | NB | W4 + CINC + GDP + MID(≥4) + Year FE | H1 & H2 with kinetic-conflict control (effective 2007–2014 because MID v4.03 ends in 2014) |
| Panel C Dataset (2007–2014) | | | |
| M5 | NB | W4 + CINC + GDP + Year FE | H1 & H2 conservative baseline (NB on clean DV) |
| M6 | ZINB | W4 + CINC + GDP + Year FE \| CINC | ZINB on clean DV |
| M7 | ZINB | W4 + CINC + GDP + Year FE \| CINC + Year FE | Primary model for H1 & H2 |

Notes: these models are described in detail in the current sub-section “Models”. The models.R script is available in the GitHub repository referenced in the Appendices section. All models include year FE. For ZINB models, the location of year FE is specified via notation: count-stage formula | inflation-stage formula (see the Hypothesis testing section for more details). All variables and data sources are reported in Tables 2 and 3.

*Robustness models overview*

I run six robustness checks (R1–R6), reported in the supplementary robustness.R script and summarised in Tables 6, 7, and 8 (see Appendices section). R1 is a re-estimation of M2 (Panel B) for a kinetic-conflict sensitivity using Militarized Interstate Disputes (Maoz et al., 2021) at any hostility level (≥1). R2 excludes the three dominant attackers (China, Russia, Iran) from Panel C. The purpose is to determine whether the H1 findings persist even after filtering out the most active autocracies.

R3–R6 re-test H1 on an entirely different dataset, the Council on Foreign Relations (CFR) Cyber Operations Tracker (Council on Foreign Relations, n.d., as cited in The Data Wrangler, 2024). It is an alternative to DCID that includes additional state-backed cyber incidents. R3, R4, R5, and R6 are mirroring the specifications of M1, M2, M3/M6 and M7 respectively. The CFR panel is monadic (it identifies the attacker but not the victim), so it tests H1 only. R6 is the primary CFR specification. Table 7 reports coefficients for the DCID-based checks (R1–R2) and Table 8 for the CFR-based checks (R3–R6).

## RESULTS

### *H1 results*

H1 is supported. Across all seven primary models, the attacker_W4 coefficient is negative and statistically significant, with magnitudes ranging from -1.96 to -5.03. Table 5 reports the full coefficient estimates. The pattern across data panels and estimators is consistent. M1 model (Panel A, most observations, with only GDP as a control) gives the largest coefficient at -5.03. Adding CINC control in M2 reduces the effect to -3.13.

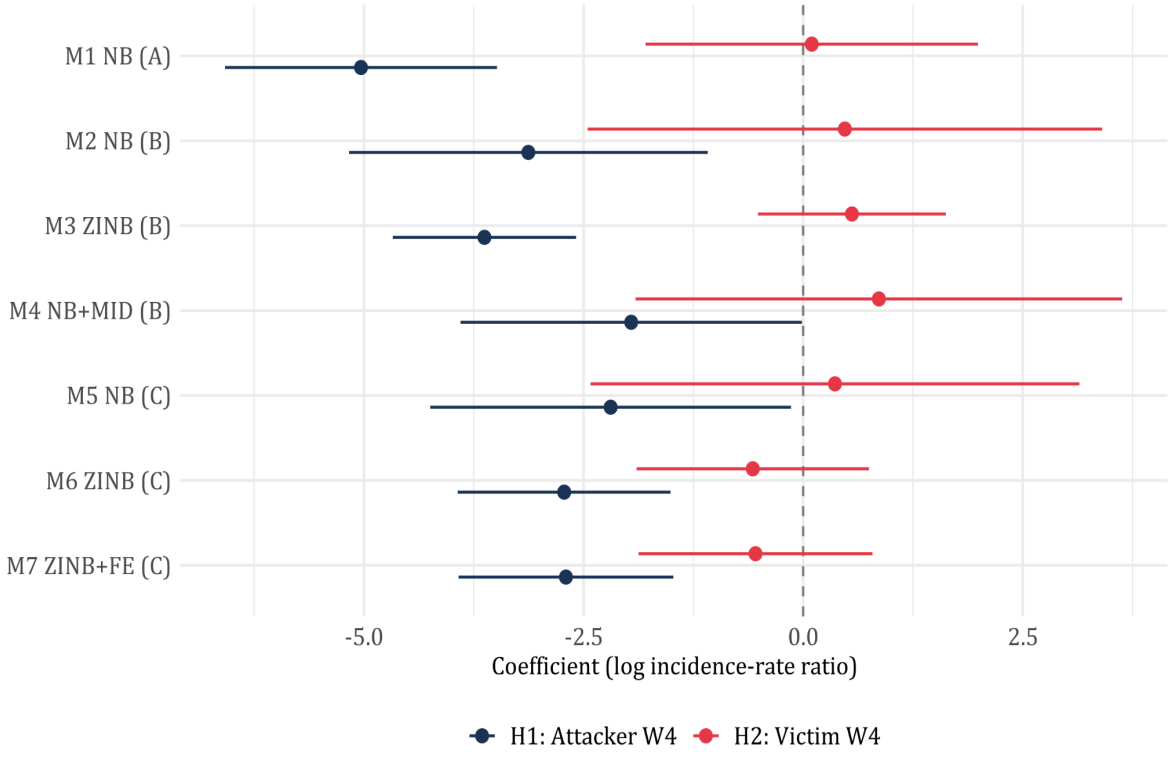
The coefficient drops further to -1.96 in M4 once a kinetic-conflict control (MID hostility $\geq$ 4) is added in Panel B. This makes theoretical sense because when two states are in active military conflict, cyber operations become an extension of that conflict rather than a reflection of the attacker's domestic politics. The MID coefficient in M4 is 6.64 ($p < 0.001$), indicating that dyad-years with active kinetic conflict have over 760 times as many cyber incidents as those without. This means that kinetic conflict is the strongest predictor of cyber operations in any model that includes it.

Panel C handles active military conflict differently. Instead of controlling for kinetic conflict, it drops such dyad-years observations from the data entirely, leaving

only purely non-kinetic cyber operations. The Panel C models (M5, M6, M7) give W4 coefficients of -2.19, -2.72, and -2.70, all statistically significant. The ZINB models (M6 and M7) have smaller standard errors because they explicitly model structural zeros.

The primary model M7 shows attacker_W4 = -2.70 ($p < 0.001$) in the count stage. Converting to an incidence-rate ratio, $\exp(-2.70) \approx 0.067$. It means a full unit increase in the attacker's winning coalition index (from 0 to 1) is associated with roughly a 93% drop in unprovoked cyber operations per dyad-year, holding everything else constant. So, an increase from a narrow-coalition state index (W4 ≈ 0.25) to a large-coalition state index (W4 ≈ 0.75) gives $\exp(0.5 \times -2.70) \approx 0.26$, a 74% drop of cyber attacks. In other words, a narrow-coalition regime is expected to conduct about four times as many unprovoked cyber operations as a broad-coalition regime against the same target, in the same year, with the same capability and wealth.

**Graph 4. Hypothesis results.**




Notes: coefficient estimates with 95% confidence intervals for the seven main models (M1–M7). ZINB models (M3, M6, M7) show count-stage coefficients. Source: own calculations. Built in R using the ggplot2 package.

The direction of the H1 finding is consistent across all 6 robustness models. The attacker_W4 coefficient is negative for all of them. However, its statistical significance is not always below the 0.05 threshold. The coefficient remains negative under the broadest kinetic control (R1, $\beta \approx -1.64$, $p \approx 0.05$). The same is observed with China, Russia, and Iran excluded (R2, $\beta \approx -2.65$, $p \approx 0.10$). The magnitudes are consistent with the main models, but the statistical significance is marginal in R1 and lost in R2. R2

retains only 31 non-zero observations, so this reflects a loss of statistical power, not a sign reversal.

I conduct the strongest robustness check of H1 in the models R3-R6, because these models test H1 on an entirely different CFR dataset (Council on Foreign Relations, n.d., as cited in The Data Wrangler, 2024). The results show that Attacker_W4 ranges from about -4.4 to -8.6 and is significant at $p < 0.01$ in all four specifications. Therefore, H1's direction is the same across all R1-R6 robustness models, and its significance is firmly supported by the CFR data. See Tables 6, 7, and 8 in the Appendices section for the full robustness results.

Taken together, the H1 results indicate that domestic political structures systematically shape a state's willingness to conduct unprovoked cyber aggression. States with broader winning coalitions, where the leadership is accountable to a larger population for the provision of public goods, conduct fewer such operations. States with smaller winning coalitions, where the leadership is accountable to a narrow elite and provides primarily private goods, conduct more cyber operations.

### *H2 results*

H2 is not supported. Across all seven primary models, the victim_W4 coefficient is statistically indistinguishable from zero, with p-values ranging from 0.31 to 0.92 and inconsistent signs across estimators (positive in M1–M5, negative in M6 and M7). When a coefficient cannot maintain its sign across specifications on the same data, the most parsimonious read is that there is no detectable underlying effect, not that the effect exists with low statistical power. The data therefore do not support the hypothesis that states with larger winning coalitions are targeted less frequently by unprovoked cyber operations.

So, the H2 results do not support the idea that regime type predicts who gets attacked in cyberspace. Instead, country material capability and wealth predict it. Victim GDP per capita is a strong positive predictor of being attacked (M7: $\beta = 0.55$, $p < 0.001$). Furthermore, victim CINC is also often a predictor of who gets targeted. The victim's winning coalition size makes no detectable difference once wealth and capability are accounted for. The robustness checks do not change the H2 results. Victim_W4 remains statistically indistinguishable from zero throughout.

**Table 5. Main models.**

| | M1 (NB, panel A) | M2 (NB, panel B) | M3 (ZINB, panel B) | M4 (NB, panel B) | M5 (NB, panel C) | M6 (ZINB, panel C) | M7 (ZINB, panel C) |
|---|---|---|---|---|---|---|---|
| Attacker W4 [H1] | -5.033*** | -3.128** (1.041) | -3.628*** (0.533) | -1.957* (0.991) | -2.191* (1.048) | -2.720*** (0.618) | -2.700*** (0.624) |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | (0.790) | | | | | | |
| Victim W4 [H2] | 0.098<br>(0.965) | 0.475<br>(1.494) | 0.555<br>(0.545) | 0.862<br>(1.413) | 0.362<br>(1.419) | -0.573<br>(0.675) | -0.542<br>(0.679) |
| Attacker CINC | | 43.195*<br>(17.533) | 76.670***<br>(12.560) | 21.082***<br>(2.558) | 24.740***<br>(5.830) | 31.012***<br>(6.574) | 32.329***<br>(7.161) |
| Victim CINC | | 27.618**<br>(9.096) | 4.017<br>(2.536) | 20.083***<br>(3.517) | 20.091***<br>(3.334) | -12.273**<br>(3.930) | -11.866**<br>(4.111) |
| Attacker ln(GDP p.c.) | 0.501*<br>(0.204) | 0.104<br>(0.146) | 0.051<br>(0.098) | 0.200<br>(0.138) | 0.202<br>(0.151) | 0.208<br>(0.112) | 0.220*<br>(0.112) |
| Victim ln(GDP p.c.) | 0.434*<br>(0.220) | 0.252<br>(0.185) | 0.085<br>(0.100) | 0.437*<br>(0.220) | 0.468*<br>(0.214) | 0.557***<br>(0.132) | 0.549***<br>(0.133) |
| MID use of force (≥4) | | | | 6.639***<br>(0.426) | | | |
| Intercept | | | -6.384***<br>(1.265) | | | -9.194***<br>(1.533) | -9.657***<br>(1.608) |
| Observations | 412118 | 295154 | 295154 | 235986 | 235864 | 235864 | 235864 |
| Non-zero obs | 205 | 136 | | 101 | 79 | | |
| % non-zero | 0.05% | 0.05% | | 0.04% | 0.03% | | |
| Total incidents | 398 | 258 | | 188 | 145 | | |
| AIC | 3837.2 | 2321.4 | 2043.8 | 1593.8 | 1345.0 | 1180.8 | 1188.1 |
| McFadden pseudo-$R^2$ | 0.0828 | 0.1711 | - | 0.2413 | 0.2074 | - | - |
| * p < 0.05, ** p < 0.01, *** p < 0.001 | | | | | | | |

Notes: all models include year fixed effects. ZINB models show count-stage coefficients only. Each model tests both H1 (attacker_w4) and H2 (victim_w4). Data source: models.R script generates outputs/tables/Table_5.html available in the GitHub repository referenced in the Appendices section.

## DISCUSSION

My research contributes to the existing academic discussion by addressing the identified literature gap of the testing of the selectorate theory in the cyberspace domain. The H1 findings support the partial applicability of the selectorate theory and the logic of political survival to cyberspace. The H1 results suggest that the size of the winning coalition predicts state-sponsored cyber aggression. The models predict the aggressive, unprovoked behaviour of narrow-coalition regimes. In the primary model (M7), a shift from a narrow-coalition regime (W4 $\approx$ 0.25) to a broad-coalition regime (W4 $\approx$ 0.75) is associated with approximately a 74% reduction in unprovoked cyber operations against the same target in the same year, controlling for capability and wealth. This finding is robust across all seven primary models, six robustness specifications, and an independent dataset.

This result extends Peceny and Butler's (2004) finding for conventional militarised disputes to a cyber domain. Peceny and Butler showed that coalition size (not the democracy/autocracy binary) predicts conflict initiation. The present study confirms that the same institutional variable predicts cyber aggression, using a continuous measure of coalition size by Bueno de Mesquita & Smith (2021). So the winning coalition effect is supported in a cyberspace characterised by low cost and high deniability. Even when the domain structurally lowers the barrier to aggression for all actors, narrow-coalition regimes still demonstrate more bellicose behaviour. While the verification of the underlying mechanism is beyond the scope of my work, the results suggest that the institutional structure, not merely the cost of an operation, drives the decision to launch the unprovoked cyber attacks.

This finding also contributes to the discussion of Smith (2019) and Shandler (2025) on whether institutional constraints extend to covert and sub-threshold state operations. Smith (2019) found that domestic elite opposition constrains even covert operations in democracies. Shandler (2025) argued that cyber operations may function differently because democratic leaders can use them without paying audience costs. The H1 results are more consistent with Smith's position. Institutional constraints appear to reduce cyber aggression in broad-coalition regimes despite the domain's low visibility. However, the effect size is smaller than that reported by Peceny and Butler (2004) for conventional disputes. And this is consistent with the possibility that cyber's low-cost nature partially weakens the institutional constraint.

The H1 results also complement Hunter et al. (2022) study of selectorate theory for cyber aggression. They found that democratic regimes have a pacifying effect on cyber aggression. The present study advances beyond their design by using a continuous regime type measure (coalition size) rather than testing using binary democracy/autocracy categories. Also this study relies on the selectorate theory, while Hunter et al. (2022) rely on the democratic peace theory in their theoretical framework.

H2 is not supported. The broad-coalition regimes are not targeted less frequently in cyberspace. This diverges from the pattern Peceny and Butler (2004) observed in conventional conflict, where broad-coalition regimes were less likely to be targeted. In the cyber domain, target selection appears driven by the value of what can be accessed or disrupted rather than by the target's institutional characteristics.

I also identified an empirical gap in current academic discussion. Modelling the state's defensive behaviour in the cyber domain needs more data to be tested. To research the mechanism by which public goods are provided through defensive cyber operations, the dataset should include a sufficient number of such observations. I manually reviewed the original DCID dataset and coded the operations by their offensive and defensive nature. However, out of ~400 cyber operations in the DCID, only 3 were unrelated to the ongoing kinetic conflict and at the same time defensive (or "hack-back") in nature: "Buckshot Yankee" (US → Russia, 2008), "NK retaliation" (North Korea → South Korea, 2011), and "Japan retaliation" (Japan → South Korea, 2010). Therefore, I identified that the current available data is largely focused on aggressive cyber operations, neglecting defensive ones.

It is important to acknowledge alternative approaches to explaining state aggression beyond the scope of this study. They often focus on individual leader characteristics, such as combat experience and other leader background (Horowitz, Stam & Ellis, 2015), or on the manner and consequences of leaders losing office (Chiozza & Goemans, 2011). These individual-level mechanisms are not tested in the present study, but they represent competing explanations that future research could examine in the cyber domain.

## PROPOSED CHANGES TO PUBLIC POLICY

The central finding of this study is that the narrow winning coalition is a plausible predictor of its state's unprovoked cyber aggression towards other states. Currently, the UK, US, EU, and Ukraine predict the likely sources of cyber aggression reactively, based on recent experience or active conventional conflict. And this is a sound approach to expect attacks from the known adversary states. However, the results of my study can also help identify other potential sources of threats. Therefore, I propose the following change for national cyber strategy policy-making.

The threat assessment should incorporate a winning coalition index, which is a structural indicator of regime type. The H1 result holds after controlling for active militarised conflict. It means that the cyber conflict is not merely a reflection of who is already at war. A narrow-coalition state is expected to conduct about four times as many unprovoked cyber operations as a broad-coalition state against the same target, in the same year, with the same capability and wealth. Policy-makers could therefore use the winning coalition index as a screen for latent threats posed by states with which their country is not currently in militarised conflict.

This approach complements rather than replaces the current reactive identification of known adversaries. It adds a forward-looking perspective on likely aggressors before a cyber incident happens. Because winning coalition sizes change over time, I recommend ongoing re-evaluation of potential adversaries rather than making a permanent list of them. This policy recommendation applies to all four cyber strategies reviewed earlier.

The second recommendation concerns Ukraine's European and Euro-Atlantic accession negotiations. Ukraine can leverage the study's findings on the relationship between cyber aggression and coalition size by arguing that it is unlikely to be the source of cyber aggression (therefore a more trustworthy partner), given its moderate-to-high winning coalition index. Over the period from 2007 to 2020, Ukraine's winning coalition index ranged from roughly 0.69 to 0.82 (Smith, 2022). This placed Ukraine's index above the most active cyber aggressors such as Russia, China, Iran, and North Korea, but below consolidated democracies such as Germany, France, and the United States (Smith, 2022). The data end in 2020, so the argument rests on Ukraine's historical trajectory rather than its current governance under martial law. The integration will likely broaden Ukraine's winning coalition, making it an even more trustworthy partner. So the winning coalition index is a measurable security argument that strengthens the case for accession on country institutional grounds.

Finally, if Ukraine eventually becomes an EU and NATO member, or its winning coalition broadens, it does not mean that Ukraine will become less or more likely a target in cyberspace. This is a direct implication of the unsupported H2. The regime's winning coalition size predicts who is likely to attack, but not who is likely to be attacked. Therefore, Ukraine cannot treat changes in the size of the winning coalition as grounds for expecting fewer or more attacks. So Ukraine's cyber strategy should assume a continuing threat from Russia (zero policy) and from other regimes with narrow or moderate-to-narrow winning coalition sizes, which the H1 result identifies as the likely attackers.

## CONCLUSIONS

I posed the following research question: "How does the size of the state's winning coalition affect its behaviour in cyberspace?" The thesis results answer this question in two ways. The regime type is a plausible predictor of attacker states, but not of targeted ones.

H1 is supported. States with broader winning coalitions conduct unprovoked cyber operations less frequently than states with narrower coalitions. Furthermore, the difference is statistically and substantively significant (see the "H1 results" subsection for the details). The result survives six robustness checks, including models on the methodologically distinct CFR dataset.

However, H2 is clearly not supported. The size of the winning coalition is not a

plausible predictor of whether a state is targeted. Instead, targeting is associated with a state's GDP per capita and material capability in military, energy, and population (CINC, Greig & Enterline, 2021). This finding suggests that the regime's institutional structure does not predict whether it will be a target of cyber aggression.

### *Data limitations*

This research has several important limitations. First, there is a lack of information about non-observed events. I work with publicly available data about the events, some of which are never to become public or never to be recognised as state-sponsored. As described earlier, countries often do not want to be associated with cyber aggression, and the nature of the cyber domain often enables them to do so. Therefore, it is important to note that the DCID dataset (Maness et al., 2022) contains only known cyber operations, while a significant share of real cyber operations remains undetected. So the thesis results should be interpreted as patterns in observed cyber aggression, which may differ from the true population of all cyber operations.

Second, the affiliation of the adversary actor with its sponsor state is often questionable. The authors of the DCID dataset recognise that the confirmation of explicitly government-sanctioned cyber campaigns is a difficult process (Maness et al., 2022, p. 2). Furthermore, upon closer review of the data, I identified some observations that are likely to be driven by non-state actors. For instance, the South Korea-Japan incidents of 2008, 2010, and 2011 (DCID v. 2.0; Maness et al., 2022) are likely to be community-driven rather than backed by the sponsor states.

The third limitation is that the number of non-zero observations in my panel data is small compared to zero-observations. It is important to highlight that, for most countries across most of the observed years, no cyber activity is available in the DCID dataset (Graph 3 clearly illustrates that). The primary Panel C covering the years 2007-2014 contains 145 incidents across 79 dyad-years, conducted by only 11 unique attacker countries. While the full Panel C dataset has 235864 observations, the signal comes from fewer than 0.04% of them. The R2 model shows that removing China, Russia, and Iran (the top 3 attackers) and leaving only 8 attackers, results in a marginal attacker W4 coefficient. The result, while robust in direction, depends on a small set of state actors. However, these limitations are not unique to my study, as any quantitative analysis of state-backed cyber operations with panel data across decades faces similar data availability constraints.

Fourth, I choose to inflate my regression-ready dataset with zeros when there is no information on whether cyber activity occurred between the given countries in a given year. On the one hand, this allows me to avoid selection bias by not ignoring the part of the population that *chooses* not to attack, even when they could. However, the zero inflation in the data also reflects structural impossibility (states that lack the capability to conduct cyber operations in a dyad-year) and observational absence (states that may conduct operations but are never caught). The ZINB models address

the former by modelling structural zeros through CINC control (Greig & Enterline, 2021), but cannot distinguish between states that chose not to attack and states whose attacks were never detected.

Fifth, the Dyadic Cyber Incident and Campaign Dataset (DCID v. 2.0; Maness et al., 2022) is constructed around the idea of dyad rivalry. As the dataset name suggests, it is designed to capture observations of incidents between state pairs, with some incidents including third parties. The original research using DCID (Valeriano & Maness, 2015) suggests that the main predictor of cyber attacks is the existing rivalry between aggressor and target states. However, the data missed many instances of "one-to-many" or "many-to-many" relationships during the observed time period. We know they existed from another publicly available source (the Council on Foreign Relations Cyber Operations Tracker). For example, CFR documented the "Regin" incident in 2014 (Council on Foreign Relations, n.d., as cited in The Data Wrangler, 2024). According to the incident description, the attack originated in the UK and the US, targeting Algeria, Afghanistan, Belgium, Brazil, Fiji, Germany, Iran, India, Indonesia, Kiribati, Malaysia, Pakistan, Syria, and Russia. There are many more similar observations in CFR, so a dedicated analysis of this dataset will be valuable for future research.

Finally, my primary dataset (Panel C) is limited to 2007-2014. The timeframe is dictated by the availability of control variables. The latest CINC data (Greig & Enterline, 2021) is available through 2016, and the latest MID dyadic data (Maoz et al., 2021) through 2014. This restricts the primary regression-ready panel (Panel C) to 2014, but the cyber domain has evolved substantially since then. While H1 in dataset Panel A (through 2020) is still supported, the results may not generalise to the period after 2014.

Despite the above limitations, the H1 finding is supported by analysing two independent datasets (DCID and CFR). All seven main specifications and six robustness checks indicate a consistent direction for the results. This is sufficient to draw the conclusion at the dyad–year level, even if absolute coverage of state-backed cyber operations remains incomplete.

### *Directions for future research*

The first direction for future research should focus on defensive state-backed cyber operations. The Dyadic Cyber Incident and Campaign Dataset (DCID v. 2.0; Maness et al., 2022) used in my thesis as a primary source of cyber observations contains only 7 cyber operations that could be classified as "active cyber defence" outside the defended cyber infrastructure (Schmitt, 2017, p. 563) (see the "Filtering out kinetic-related cyber operations" subsection for details and Table 9 in the Appendices section). Therefore, DCID contains too few observations for analysis of defensive state-backed cyber operations. Based on the selectorate theory, the H3 hypothesis could be "The larger the regime's winning coalition, the higher the

likelihood of conducting defensive state-backed cyber operations". We would expect democracies to be willing to provide public goods in the form of cyber defence. This would complement research on selectorate theory, similarly to Adamson's (2020) study on defence battles as a public good.

Another interesting direction of further research is the unprovoked cyber aggression explicitly between states with a broad winning coalition. The only democracy-on-democracy (attacker_w4 > 0.75, victim_w4 > 0.75) observations in the DCID dataset are incidents between South Korea and Japan in 2008, 2010, and 2011 (DCID v. 2.0; Maness et al., 2022). They are traceable to a hacktivist campaign with no documented state sponsorship, suggesting a coding ambiguity in the dataset rather than state-backed aggression. However, the alternative dataset, the Council on Foreign Relations (CFR) Cyber Operations Tracker (n.d.), documents cases of capable democracies conducting cyber espionage against allied democratic states. Examples include French intelligence operations targeting NATO partners ("Snowglobe" operation, 2014), Spanish intelligence targeting EU member governments ("Careto" operation, 2014), and US/UK operations touching German infrastructure ("Regin" operation, 2014) (Council on Foreign Relations, n.d., as cited in The Data Wrangler, 2024). These cases, which include espionage between formal allies, are not covered in DCID 2.0 (Maness et al., 2022). So, future research should test whether the winning coalition, as selectorate theory suggests, acts as an institutional constraint in cyberspace, preventing democracies from targeting each other.

## REFERENCES

Adamson, J. (2020). Political institutions, resources, and war: Theory and evidence from ancient Rome. Explorations in Economic History, 76, 101324. https://doi.org/10.1016/j.eeh.2020.101324

Adler, E., & Barnett, M. (Eds.). (1998). *Security communities*. Cambridge University Press.

Baldwin, D. A. (Ed.). (1993). *Neorealism and neoliberalism: The contemporary debate*. Columbia University Press.

Bank of Korea. (n.d.). *Bank of Korea*. Retrieved March 28, 2026, from https://www.bok.or.kr/eng/main/main.do

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. International Affairs, 96(3), 749–766.

Bueno de Mesquita, B., Smith, A., Siverson, R. M., & Morrow, J. D. (2003). *The logic of political survival*. MIT Press.

Bueno de Mesquita, B., & Smith, A. (2021). A New Indicator of Coalition Size: Tests Against Standard Regime-Type Indicators. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3925591

Chapple, M., & Seidl, D. (2021). *Cyberwarfare: Information operations in a connected world*. Jones & Bartlett Learning.

Chiozza, G., & Goemans, H. E. (2011). *Leaders and international conflict*. Cambridge University Press.

Clarke, K. A., & Stone, R. W. (2008). Democracy and the logic of political survival. *American Political Science Review*, *102*(3), 387–392.

Coppedge, M., Gerring, J., Knutsen, C. H., Lindberg, S. I., Teorell, J., Alizada, N., ... & Ziblatt, D. (2021). *V-Dem dataset v11.1* [Data set]. Varieties of Democracy Project. https://www.v-dem.net/data

Correlates of War Project. (n.d.). *COW country codes* [Data set]. Retrieved March 28, 2026, from https://correlatesofwar.org/data-sets/cow-country-codes-2/

Council on Foreign Relations. (n.d.). *Cyber operations tracker*. Retrieved May 17, 2026, from https://www.cfr.org/cyber-operations/

Council of the European Union. (2024). *Cyber sanctions*. https://www.consilium.europa.eu/en/policies/sanctions-against-cyber-attacks/

Debs, A., & Goemans, H. E. (2010). Regime type, the fate of leaders, and war. *American Political Science Review*, *104*(3), 430–445.

Diehl, P. F., & Goertz, G. (2000). *War and peace in international rivalry*. University of Michigan Press.

Dong, J., Chen, S., Ding, F., Zhuo, J., & Hao, M. (2025). Spatiotemporal characteristics and drivers of global cyber conflicts. *Humanities and Social Sciences Communications*, *12*(1), 665. https://doi.org/10.1057/s41599-025-04897-7

Doyle, M. W. (2005). Three pillars of the liberal peace. *American Political Science Review*, *99*(3), 463–466.

Ebert, H., & Maurer, T. (2013). Contested cyberspace and rising powers. *Third World Quarterly*, *34*(6), 1054–1074.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. (2020). *The EU's cybersecurity strategy for the digital decade*

(JOIN(2020) 18 final). https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy

Finnemore, M. (1996). *National interests in international society*. Cornell University Press.

Gallagher, M. E., & Hanson, J. K. (2015). Power tool or dull blade? Selectorate theory for autocracies. *Annual Review of Political Science*, *18*, 367–385. https://doi.org/10.1146/annurev-polisci-071213-041224

Geddes, B. (1999). What do we know about democratization after twenty years? *Annual Review of Political Science*, *2*(1), 115–144.

Gerstle, G. (2018). The rise and fall (?) of America's neoliberal order. *Transactions of the Royal Historical Society*, *28*, 241–264.

Gilpin, R. (1981). *War and change in world politics*. Cambridge University Press.

Green, J. A. (Ed.). (2015). *Cyber warfare: A multidisciplinary analysis*. Routledge.

Greig, J. M., & Enterline, A. J. (2021). *National material capabilities (NMC) data* (Version 6.0) [Data set]. Correlates of War Project. https://correlatesofwar.org/data-sets/national-material-capabilities/

HM Government. (2022). *Government cyber security strategy 2022–2030*. https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf

Horowitz, M. C., Stam, A. C., & Ellis, C. M. (2015). *Why leaders fight*. Cambridge University Press.

Hunter, L., Albert, C., Garrett, E., & Rutland, J. (2022). Democracy and cyberconflict: How regime type affects state-sponsored cyberattacks. *Journal of Cyber Policy*, *7*(1), 1–23. https://doi.org/10.1080/23738871.2022.2041060

Kastner, J., & Wohlforth, W. C. (2025). *A measure short of war: A brief history of great power subversion*. Oxford University Press.

Keohane, R. O. (2005). *After hegemony: Cooperation and discord in the world political economy* (Rev. ed.). Princeton University Press.

Keohane, R. O., & Nye, J. S. (1973). Power and interdependence. *Survival*, *15*(4), 158–165.

Maness, R. C., Valeriano, B., Hedgecock, K., Jensen, B. M., & Macias, J. M. (2022). *The Dyadic Cyber Incident and Campaign Dataset* (Version 2.0) [Data set]. https://www.ryanmaness.com/cyber-conflict-dataset

Maoz, Z., Johnson, P. L., Kaplan, J., Ogunkoya, F., & Shreve, A. (2018). The dyadic militarized interstate disputes (MIDs) dataset version 3.0: Logic, characteristics, and comparisons to alternative datasets. *Journal of Conflict Resolution*. https://doi.org/10.1177/0022002718784158

Maoz, Z., Johnson, P. L., Kaplan, J., Ogunkoya, F., & Shreve, A. (2021). *Dyadic MID dataset* (Version 4.03) [Data set]. Correlates of War Project. https://correlatesofwar.org/data-sets/mids/

Mearsheimer, J. J. (2001). *The tragedy of great power politics*. W. W. Norton.

Morgenthau, H. J. (1948). *Politics among nations: The struggle for power and peace*. Alfred A. Knopf.

Mueller, M. L. (2010). *Networks and states: The global politics of Internet governance*. MIT Press.

Nye, J. S. (1992). What new world order? *Foreign Affairs*, *71*(2), 83–96.

Onuf, N. G. (1998). World politics in a new key. Rowman & Littlefield.

Palmer, G., D'Orazio, V., Kenwick, M., & Lane, M. (2015). The MID4 data set, 2002–2010: Procedures, coding rules, and description. *Conflict Management and Peace Science*, *32*(2), 222–242.

Peceny, M., & Butler, C. K. (2004). The conflict behavior of authoritarian regimes. *International Politics*, *41*(4), 565–581.

Poznansky, M. (2019). Feigning compliance: Covert action and international law. *International Studies Quarterly*, *63*(1), 72–84.

Quinn, R., & Gibson, B. (2017). *An analysis of Kenneth Waltz's Theory of International Politics*. Macat Library.

Reiter, D., & Stam, A. C. (2002). *Democracies at war*. Princeton University Press.

Rosato, S. (2003). The flawed logic of democratic peace theory. *American Political Science Review*, *97*(4), 585–602.

Rosenberger, L. (2020). Making cyberspace safe for democracy. *Foreign Affairs*, *99*(3), 146–159.

Ruggie, J. G. (1998). *Constructing the world polity: Essays on international institutionalization*. Routledge.

Schmitt, M. N. (Ed.). (2017). *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.

Schweller, R. L. (1994). Bandwagoning for profit: Bringing the revisionist state back in. *International Security*, *19*(1), 72–107.

Shandler, R. (2025). Cyber conflict & domestic audience costs. *International Interactions*, 1–25. https://doi.org/10.1080/03050629.2025.2478145

Singer, J. D., Bremer, S., & Stuckey, J. (1972). Capability distribution, uncertainty, and major power war, 1820–1965. In B. Russett (Ed.), *Peace, war, and numbers* (pp. 19–48). Sage.

Slobodian, Q. (2018). *Globalists: The end of empire and the birth of neoliberalism*. Harvard University Press.

Smith, A. (2022). *Replication data for: A new indicator of coalition size* (Version 1) [Data set]. Harvard Dataverse. https://doi.org/10.7910/DVN/UYLXRO

Smith, G. L. (2019). Secret but Constrained: The Impact of Elite Opposition on Covert Operations. International Organization, 73(3), 685–707. https://www.jstor.org/stable/26758062

Taiwan Directorate-General of Budget, Accounting and Statistics. (n.d.). *Macro database*. Executive Yuan, Republic of China (Taiwan). Retrieved March 28, 2026, from https://nstatdb.dgbas.gov.tw/dgbasall/webMain.aspx?k=engmain

The Data Wrangler [justin2028]. (2024). *State-sponsored cyber operations (2005–present)* [Data set]. Kaggle. https://www.kaggle.com/datasets/justin2028/state-sponsored-cyber-operations-2005-present

The White House. (2026). *President Trump's cyber strategy for America*. https://www.whitehouse.gov/wp-content/uploads/2026/03/president-trumps-cyber-strategy-for-america.pdf

The World Bank. (n.d.). *World development indicators* [Data set]. Retrieved from https://databank.worldbank.org/source/world-development-indicators

Tsagourias, N. (2012). Cyber attacks, self-defence and the problem of attribution. *Journal of Conflict and Security Law*, *17*(2), 229–244.

Valeriano, B., & Maness, R. C. (2014). The dynamics of cyber conflict between rival antagonists, 2001–11. *Journal of Peace Research*, *51*(3), 347–360.

Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.

Walt, S. M. (1990). *The origins of alliances*. Cornell University Press.

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.

Weeks, J. L. P. (2014). *Dictators at war and peace*. Cornell University Press.

Wendt, A. (1992). Anarchy is what states make of it: The social construction of power politics. *International Organization*, *46*(2), 391–425.

Wendt, A. (1999). *Social theory of international politics*. Cambridge University Press.

Whyte, C., & Mazanec, B. M. (2023). *Understanding cyber-warfare: Politics, policy and strategy* (2nd ed.). Routledge.

Кабінет Міністрів України. (2025). *Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України* (Розпорядження № 204-р від 7 березня 2025 р.). https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text

Президент України. (2021). *Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України"* (Указ № 447/2021). https://zakon.rada.gov.ua/laws/show/447/2021

## APPENDICES

Project source code is available via GitHub repository:
https://github.com/mklovak/regimes-cyber-operations/tree/main

All model results and tables are available in the same git repository in the folder outputs/tables:

https://github.com/mklovak/regimes-cyber-operations/tree/main/outputs/tables

README.md:
https://github.com/mklovak/regimes-cyber-operations/blob/main/README.md

| Table 6. Robustness Models Overview (R1-R6) | | | | |
|---|---|---|---|---|
| Model | Category | Estimator | Panel | Specification |
| R1 | Kinetic-conflict sensitivity | NB | B (2007-2014) | M2 + MID at any hostility (>=1) |
| R2 | Dominant-attacker exclusion | NB | C (2007-2014) | M5 excluding China, Russia, Iran |
| R3 | CFR alternative dataset | NB | CFR A (2007-2020) | Monadic; W4 + GDP; year FE |
| R4 | CFR alternative dataset | NB | CFR B (2007-2016) | Monadic; W4 + CINC + GDP; year FE |
| R5 | CFR alternative dataset | ZINB | CFR B (2007-2016) | Monadic ZINB; year FE in count stage |
| R6 | CFR alternative dataset | ZINB+FE | CFR B (2007-2016) | Monadic ZINB; year FE in both stages (primary CFR) |

Notes: all models include year fixed effects. Each model tests both H1 (attacker_w4) and H2 (victim_w4). Data source: robustness.R script generates outputs/tables/Table_6.html available in the GitHub repository referenced in the Appendices section.

| Table 7. Robustness Checks on the DCID Data (R1-R2). | | |
|---|---|---|
| | R1 NB+MID-any (B) | R2 NB excl. top-3 (C) |
| Attacker W4 [H1] | -1.642<br>(0.853) | -2.650<br>(1.597) |
| Victim W4 [H2] | 1.324<br>(1.293) | -0.314<br>(4.348) |
| Attacker CINC | 18.343***<br>(2.441) | 45.363**<br>(15.423) |
| Victim CINC | 20.344***<br>(3.332) | 29.263<br>(43.015) |
| Attacker ln(GDP p.c.) | 0.135<br>(0.146) | 0.164<br>(0.592) |
| Victim ln(GDP p.c.) | 0.239<br>(0.207) | 0.191<br>(0.293) |

| | | |
|---|---|---|
| MID any hostility (≥1) | 6.354***<br>(0.363) | |
| Observations | 235986 | 231786 |
| Non-zero obs | 101 | 31 |
| % non-zero | 0.0428% | 0.0134% |
| Total incidents | 188 | 44 |
| AIC | 1407.4 | 601.6 |
| * p < 0.05, ** p < 0.01, *** p < 0.001 | | |

Notes: all models include year fixed effects. R1: M2 + MID at any hostility (>=1), Panel B, effectively 2007-2014. R2: M5 excluding China, Russia and Iran, Panel C. Dyad-clustered SEs. Each model jointly reports H1 (attacker_w4) and H2 (victim_w4). Data source: robustness.R script generates outputs/tables/Table_7.html available in the GitHub repository referenced in the Appendices section.

**Table 8. Robustness Checks on the CFR Data (R3-R6, H1 only)**

| | R3 CFR NB (A) | R4 CFR NB (B) | R5 CFR ZINB (B) | R6 CFR ZINB+FE (B) |
|---|---|---|---|---|
| Attacker W4 [H1] | -8.617***<br>(1.466) | -4.635**<br>(1.500) | -4.694***<br>(1.020) | -4.435***<br>(1.062) |
| Attacker CINC | | 52.976<br>(47.477) | 5.819<br>(3.004) | 6.698<br>(3.772) |
| Attacker ln(GDP p.c.) | 1.231***<br>(0.268) | 0.433<br>(0.259) | 0.425<br>(0.230) | 0.357<br>(0.238) |
| Intercept | | | -1.924<br>(1.645) | -1.670<br>(1.654) |
| Observations | 2409 | 1723 | 1723 | 1723 |
| Non-zero obs | 94 | 49 | 49 | 49 |

| | | | | |
|---|---|---|---|---|
| % non-zero | 3.90% | 2.84% | 2.84% | 2.84% |
| Total incidents | 455 | 163 | 163 | 163 |
| AIC | 1081.0 | 519.5 | 431.1 | 441.6 |
| * p < 0.05, ** p < 0.01, *** p < 0.001 | | | | |

Notes: Monadic country-year panel from the CFR Cyber Operations Tracker. All models include year fixed effects: in the linear predictor for NB models (R3, R4); in the count stage for R5; in both stages for R6. Country-clustered SEs for NB models. Model-based SEs for ZINB models. H2 is not tested on CFR (no victim information). R6 is the primary CFR specification, mirroring M7 in the DCID main analysis. Data source: robustness.R script generates outputs/tables/Table_8.html available in the GitHub repository referenced in the Appendices section.

**Table 9. Manually coded defensive/retaliatory cyber operations excluded from Panel C.**

| Operation name | Attacker → Victim | Coding justification |
|---|---|---|
| Buckshot Yankee (non-kinetic) | US → Russia | US defensive response to Russian intrusion |
| Osinform | Georgia → Russia | Georgia retaliating against Russian hackers |
| November 2008 defacements_B | Pakistan → India | Pakistan retaliating for Indian defacement |
| Japan retaliation (non-kinetic) | Japan → South Korea | Japan retaliating for South Korean DDoS |
| September 2010 defacements 2 | India → Pakistan | India retaliating for Pakistani defacements |
| PCA retaliation | India → Pakistan | India retaliating for Pakistani defacements |
| NK retaliation (non-kinetic) | North Korea → South Korea | NK retaliating for anti-Kim cyber disruption |

Notes: operations identified through manual review of the Political Objective field in DCID v. 2.0 (Maness et al., 2022). Classification follows the Tallinn Manual 2.0

definition of active cyber defence (Schmitt, 2017, pp. 563–565). Source: data_preparation.R, lines defining acd_names.