Hacking elections:
A quantitative analysis of cyber-enabled foreign election interference

Gregg R. Murray*
Craig Douglas Albert
Jeffery T. Bates
Kendyll Pfeifer

MA in Intelligence and Security Studies Program
Department of Social Sciences
Augusta University
1120 15th St.
Augusta, GA 30912 USA

While there are many individual case studies of foreign election interference in the form of cyber-enabled attacks on elections and electoral institutions, there are few if any quantitative studies of this disruptive phenomenon. This study quantitatively analyzes 85 cyber-enabled foreign attacks on elections and electoral systems worldwide between 2014 and 2020. The cases include various attackers as well as attack vectors such as denial-of-service attacks, cyber operations, influence operations, and information warfare and disinformation. The 34 targeted countries span multiple regions and vary by national power, economic status, government type, and other political and social measures. The analysis is intended to identify characteristics of countries that make them more or less vulnerable to this form of attack.

* Corresponding author: gmurray@augusta.edu

Acknowledgements: The authors thank Carter Rhea for guidance regarding machine learning.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

INTRODUCTION

Cyberspace's rapid growth has revolutionized global politics, especially concerning the issues of security and governance. States increasingly see cyberspace as strategically important, weaponizing it for both attack and defense due to growing digital reliance. Foreign election interference (FEI) involves intentional attempts by state or non-state actors to influence elections in other countries (Ohlin 2020). FEI can include cyberattacks, voter suppression, disinformation campaigns, and manipulation of social media platforms (Hansen and Lim 2019; Stedmon 2020). In an increasingly digitally dependent global society, cyber-enabled FEI (CFEI) has become a key concern to democracies worldwide as cyber technology and threats become more sophisticated. While there are many individual case studies of foreign election interference in the form of cyber-enabled attacks on elections and electoral institutions (Hansen and Lim 2019; Manwaring and Holloway 2023; Vićić and Gartzke 2024) the purpose of this paper is to identify the characteristics of countries that make them more or less likely to be targets of cyber-enabled attacks on their elections and electoral institutions. Accordingly, this study lays the groundwork for future research that seeks to broadly understand CFEI, including both targets and attackers.

This paper proceeds in four main sections. First, a review of the relevant literature provides background on this topic by exploring the militarization of cyberspace and how the internet has become both a territorial domain and a battlefield for modern warfare. The literature review also explores the overall ambiguity and challenges that current legal frameworks face when state and non-state actors reach across international lines and threaten independent political processes. Second, this paper employs a quantitative analysis, primarily based on machine learning, of 85 attacks across 34 countries between 2014 and 2020, and presents the data and methods used to perform comparative analyses. Third, the results of the analyses are presented, to include identifying common patterns and characteristics of targeted states. This paper ends with a discussion and conclusion section to analyze

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

the recurring themes found in the data that aid in understanding why certain countries are more or less vulnerable to CFEI.

LITERATURE REVIEW

Strategic Goals in Cyberspace

The evolution of technology, accompanied by the Internet of Things (IoT), has significantly transformed how future wars will be fought and won, pushing the boundaries of traditional warfare by integrating cyber capabilities. As cyber capabilities evolved, it did not take long for military planners to come to the "realization that cyberspace, like the physical world, also has military and strategic dimensions" (Attatfa et al. 2020, 60). As Ohlin and Hollis (2021) state, the internet is increasingly weaponized, with states using sophisticated cyber campaigns to pursue strategic goals without direct military engagement. This has been greatly exacerbated due to the limitless nature of cyberspace, where boundaries are not defined by geography, and digital footprints are difficult to trace. This alone has challenged the traditional concepts of warfare, as many of the actors involved are no longer confined to nation-states but also include non-state actors that influence the geopolitical landscape. It also becomes a problem of attribution due to factors such as location, identity, and the difficulty in determining the actors involved (Brantley and Smeets 2020). This has provided a "cloak-and-dagger" approach, providing flexibility for state actors who often claim plausible deniability.

As the cyber domain continues to evolve, the ambiguity surrounding actions taken in cyberspace poses challenges for international law and norms, raising questions about how to effectively regulate and respond to cyber threats in a rapidly changing world. This often creates a "common notion that low barriers of entry create a diffusion of cyber-power, or that the invisible nature of cyber weapons makes it difficult to govern" (Gorwa and Smeets 2019, 15). This blending of traditional and cyber warfare signals a shift in how global power dynamics shape and how national security concerns will be shaped in

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

the future. The strategic value of cyberwarfare has presented nation-states with new opportunities and challenges in the realm of modern conflict. This has opened a Pandora's box, where the potential for both innovation and destruction exists in equal measures. In its existential form, strategic capabilities can create an overarching effect, but as Kallberg (2016, 115) notes, “cyber lacks the feedback loop of quantifiable results and with limited measure of effectiveness.” Though limitations are implied, it does affect how nation-states form national security strategies. It presents clear boundaries but does not stop aggressors from trying to exploit cyberspace for a strategic advantage, challenging traditional notions of communication, security, and law.

Pursuing strategic goals in cyberspace creates significant risks, as misunderstandings and misperceptions may push states toward unintended escalations. As Slayton (2017, 73) states, “cyber operations can blur lines between espionage (or “cyber exploitation”) and use of force (or “cyber attack”), they create a cybersecurity dilemma.” In this domain, where the speed of action often outpaces traditional diplomatic responses, the lines between defensive and offensive cyber operations can blur, complicating the assessment of intent and capabilities. Consequently, states may respond to perceived threats with disproportionate measures, leading to a cycle of tension. Dunn-Cavelty (2014, 701) explains that current approaches to cyber-security strategies are proving ineffective, resulting in diminished security, as the issue is complex and extends beyond the traditional scope of state-to-state relations. As security diminishes, uncertainty increases, fostering fear and leading to the emergence of a self-help system, aligning with a realist perspective ultimately prioritizing self-interest above all else.

The absence of geographical boundaries or markers in cyberspace creates a unique challenge for states seeking to assert sovereignty and control. Keitner (2020) notes, the fundamental understandings of the characteristics and rights of states in the international system are reflected in the principles of sovereignty, territorial integrity, political independence, self-determination, and nonintervention. Due to the unregulated vastness of cyberspace, states face unprecedented challenges in maintaining control

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

over their digital environments. With no single point of control, cyberspace enables free and unfiltered communication, resulting in decentralization, making regulation difficult.

Foreign Election Interference

Elections are fundamental to democracies. Questions of elections' legitimacy can erode public trust, deepen divisions within society, and weaken a state's capacity to govern. As Marshall Palmer and Wilner (2025, 9) explain, the weaponization of delegitimization turns on social pressure and perceptions of right and wrong, leveraging an actor's normative, ethical, or ideological perspective to constrain behavior. By targeting the legitimacy of key state functions, such as election, adversaries can gradually destabilize fragile systems and processes. Understanding those vulnerabilities allows states to better prepare for contingencies.

The inability to reign in foreign interference has been a long-standing issue as foreign actors have sought to destabilize democratic institutions or political processes that threaten their strategic interests. The internet and cyberspace have allowed unfettered access into most systems and societies. It has also led to a "growing concern about the degree to which digital media and device networks can be used as tools of social control" (Shorey and Howard 2016, 1). In this context, the degree of vulnerability is important. Various factors contribute to vulnerability, including the integrity of a country's digital infrastructure, the level of awareness regarding misinformation, legal frameworks, political stability, and the robustness of a country's cybersecurity measures. The effectiveness of election interference has been amplified by technological advances enabling cyber activities to expand leaving most countries vulnerable to new and increasingly sophisticated threats. These advances create challenges in safeguarding democratic processes, requiring security measures to evolve constantly. As Shackelford et al. (2020, 1750) explain, preserving the Republic for the next century calls for a variety of policy responses, ranging from controlling the most extreme abuses of online platforms to protecting

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

the voting process itself and preventing both domestic and international actors from undermining democratic institutions, both online and offline.

Social media platforms, with their ability to rapidly disseminate information to wide audiences, have provided adversaries with a tactical and strategic platform for foreign influence operations. Tucker et al. (2018, 4) state social media usage has the potential to drive political polarization when disinformation is prevalent, thereby affecting democratic quality (4). Whyte (2020, 2) also argues that democratic election interference goes beyond computer network exploitation techniques and primarily entails the pervasive manipulation and compromise of the algorithmic structure of information platforms, which now determine how information is circulated in democracies. A clear example can be seen during Taiwan's 2020 national election, as a disinformation campaign, allegedly from mainland China, aimed to disrupt the electoral process (O'Conner et al. 2020, 28). The *Guardian* reported that AI-generated fake news spread rapidly on social media, while fake accounts and trolls flooded posts with pro-China content and comments. The goal was to manipulate online search algorithms and create confusion, undermining democracy. Russian meddling in the US 2016 presidential election is another example, "where automated accounts promoted both white supremacist and Black Lives Matter content, sharpening polarization on both sides of the debate" (Schia and Gjesvik 2020, 415). These examples give insight into how manipulation and disinformation are actively employed in online spaces to influence elections and public opinion. Election interference has become a growing concern for democracies across the globe. The central issue then becomes maintaining the integrity of political systems and determining the best way to protect them. Understanding those characteristics is essential for safeguarding the integrity of democratic processes worldwide.

The strength and sophistication of a country's digital infrastructure are among the most crucial factors determining its vulnerability to election interference. As elections increasingly rely on digital platforms for voting, voter registration, and dissemination of electoral information, weak or outdated

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

infrastructure presents a significant risk. As Asevameh et al. (2024, 233) explain, the urgent necessity for all-encompassing measures to safeguard election integrity have been highlighted by high-profile instances of electoral infrastructure breaches in the United States and other nations. The lack of deterrence measures has left systems vulnerable to manipulation or sabotage, leaving a country with limited options for response. These options are constrained by insufficient funding, as upgrading digital infrastructure often requires significant financial resources.

Even if countries muster the financial resources to fund such efforts, Marshall Palmer and Wilner (2024, 7) argue bad actors will still hold significant capacity to influence foreign elections as emerging technologies like blockchain, cryptocurrencies, social media, and AI-generated content enable new methods for funding, creating, and distributing election influence. Cyberattacks have also become a major threat to the integrity of elections worldwide, as they can disrupt voting processes and erode public trust in democratic systems. These attacks often target critical infrastructure, such as voter databases, with the intent to manipulate or modify election-related content. An example of this occurred ahead of Indonesia's 2019 election, when Russian and Chinese hackers sought to undermine the electoral process by attacking the nation's voter database to create fake voter identities, known as "ghost voters" (Hanson et al. 2019, 19). As the complexity of modern threats evolves, and adversaries use more sophisticated tools and methods, state-sponsored tactics will make it difficult to anticipate future interference.

DATA & METHODS

Data.

To explore the conditions under which countries experience CFEI, this study examines a broad array of political, social, and economic measures for countries that were and were not victims of CFEI. Instead of being constrained by extant theories regarding this topic, of which there are few, we employ

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

a machine learning approach to identify patterns and relationships that may be overlooked by current approaches. This study is based on a panel dataset of worldwide CFEI events, which serve as the dependent variable. Appendix A reports the countries targeted, the year of the attack, the attacker, and the attack vector. We augment those data with political, social, and economic measures covering all countries globally, attacked or not, from 2014 to 2020 as recognized by the World Bank. This allows a comparison across several factors of countries that were and were not attacked.

The dependent variable is occurrences of CFEI reported by the Australian Strategic Policy Institute's International Cyber Policy Centre (ASPI-ICPC; O'Connor et al., 2020). The ASPI-ICPC compiles systematic records of state-sponsored cyber operations targeting electoral processes. The dependent variable is operationalized as an indicator variable, TARGETED, coded 1 if any CFEI activity occurred in a country-year, and 0 otherwise. ASIP-ICPC claims that CFEI "[has] been used to seek to influence voters and their turnout at elections, manipulate the information environment and diminish public trust in democratic processes" (O'Connor et al., 2020, 7). It defines CFEI as using cyber-enabled techniques to interfere in elections and referenda via two types of cyber activity:

1. Cyber operations: covert activities carried out via digital infrastructure to gain access to a server or system in order to compromise its service, identify or introduce vulnerabilities, manipulate information or perform espionage (e.g., confuse, mislead and manipulate targets through deceptive or inaccurate information (2));
2. Online information operations: information operations carried out in the online information environment to covertly distort, confuse, mislead and manipulate targets through deceptive or inaccurate information (e.g., exploit the digital presence of election campaigns, politicians, journalists, and voters (2)).

Country-year is the unit of analysis. The dataset starts with 1519 country-years with seven observations on 216 countries. O'Connor et al. logically removed from the dataset of CFEI events all

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

countries reported as “Not Free” in the Freedom House ratings of political freedom (Freedom House, 2021) as these countries do not have legitimate elections worth interfering with. We did this same in the dataset used here, which reduced the number of country-years to 1005.

This is an exploratory analysis, so the preliminary set of independent variables includes a broad array of common political, social, and economic measures obtained from publicly available sources. The political variables include measures of democracy (Polity and Freedom House scores), governance capacity (Stateness), and geopolitical power and rivalry. The social covariates include population, global region, and life expectancy. The economic indicators include measures of GDP, unemployment, and military expenditures. These data are primarily sourced from the World Bank and related cross-national repositories. All data are publicly accessible and reported in Appendix B.

Table 1 presents comparisons of country-years that were the subject of CFEI and those that were not. The table indicates there are far more country-years and unique countries that were “Not Targeted” (96%) than “Targeted” (4%). Despite the concern that CFEI evokes, this suggests it is relatively infrequent.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Table 1.	Targeted	Not Targeted
Countries	34 (18%)	151 (82%)
Country-years	38 (4%)	967 (96%)
Life Expectancy (yrs)*	77.6	72.7
Population (millions)*	76.4	31.8
Population, % Urban*	74.4	59.2
Unemployment %	8.1	7.5
GDP ($, trillions)*	2.99	0.33
GDP per capita*	28,336	15,919
Women in Parliament %*	26.7	21.8
POLITY2 (level of democracy)	8.2	7.2
FH Total (political freedom)*	80.1	73.6
Freedom of Press	74.3	72.9
Stateness*	0.82	0.73
Military Expenditures %*	2.0	1.6
Militarization (GMI)*	122.8	99.5
World Power (WPI)*	0.66	0.43

* difference $p < 0.05$

Socio-demographically, country-years experiencing CFEI had significantly higher life expectancy (77.6 years) compared to those that did not (72.7 years). This suggests that more developed, potentially stable nations are more likely to be targeted. Targeted country-years have significantly larger populations (76.4 million) than non-targeted countries (31.8 million). Larger countries might be seen as higher-value targets that have more geopolitical influence. Targeted country-years have a significantly higher percentage of urban population (74.4%) compared to non-targeted countries (59.2%). Urbanization may increase a country's digital footprint and vulnerability.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Economically, there's a slight, though not statistically significant, difference in unemployment rates, with targeted country-years having a slightly higher rate. Targeted country-years have significantly larger GDPs ($2.99 trillion) than non-targeted countries ($0.33 trillion). And targeted country-years have significantly higher GDP per capita ($28,336) than non-targeted countries ($15,919). This reinforces the idea that economically powerful and wealthier nations are more likely to be targeted.

Politically, targeted country-years are more democratic per POLITY2 and Freedom House total political freedom scores and there is a slight but not statistically significant difference in freedom of the press. Targeted country-years have a significantly higher percentage of women in parliament (26.7%) than non-targeted countries (21.8%). This might indicate that more democratic or progressive nations are being targeted. Further, targeted country-years have significantly higher STATENESS scores, suggesting they have stronger and more effective state institutions.

Finally, targeted country-years have significantly higher military expenditures as a percentage of GDP (2.0%) than non-targeted countries (1.6%), greater militarization (GMI), and significantly greater geopolitical power WPI (0.66) than non-targeted countries (0.43). Together these suggest that greater military power is associated with a higher probability of being targeted with CFEI.

In summary, Table 1 suggests country-years targeted with CFEI are generally wealthier and more economically powerful, more developed with higher life expectancy and urbanization, more democratic with greater political freedoms, more militarized and powerful on the world stage, and more populous.

Methods.

As this study is designed to explore a wide range of factors that may be related to CFEI, we use machine learning to uncover relationships. More specifically, we use a random forest (RF) classifier. RF classification is a supervised machine learning algorithm that combines multiple decision trees to build a predictive model. This multi-model aggregation process is intended to improve predictive accuracy and

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

reduce overfitting. Each tree is built using a random subset of the data via bootstrapping and a random subset of variables at each split, which creates a heterogeneous "forest" of trees. For final classification, each tree "votes" on the predicted class or value of the dependent variable, and the final classification decision is determined by the majority vote across all trees.

RF classification is considered a robust method of estimation. It has the capacity to analyze large datasets with many variables and the ability to estimate both linear and non-linear relationships. That said, the results are less interpretable than simpler models like single decision trees or regression equations, so random forest classification requires additional analyses to report the strength and direction of relationships between the dependent and independent variables.

The data were split randomly into training and test sets. In line with machine learning convention, the models were trained or built on 70% of the country-years and then tested for robustness on the remaining 30% of country-years. We used the caret package in R to implement the random forest algorithm (Kuhn, 2008). The random forest algorithm was instructed to build 500 CART (Classification and Regression Tree) models. During model training, the algorithm applied repeated five-fold cross-validation, repeated three times, to evaluate performance. Each tree in the forest is grown using bootstrapped samples of the training data. At every split, the model randomly selected a subset of 10 independent variables before choosing the best split. For classification tasks, the trees use the Gini Index as the splitting criterion, favoring splits that create purer nodes, which are more homogenous in terms of the predicted outcome. Finally, the robustness of the model to generalize to new, unseen data is checked using the test data.

As a note, while the RF classifier is robust to data conditions, extremely unbalanced data can bias model results. In this case, the dependent variable, TARGETED, is severely imbalanced. There are only 38 country-years (4%) of the 1005 country-years with CFEI. Therefore, we used the Synthetic Minority Oversampling Technique (SMOTE) as implemented in the smotefamily package in R

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

(Siriseriwan, 2024) to oversample the country-years with CFEI to balance the dataset. SMOTE works by creating synthetic samples of the minority or underrepresented outcome (i.e., targeted cases). To do this, it selects a minority observation and generates new points along the line between that observation and its nearest minority neighbors. This approach helps balance the training data, which allows models to better learn patterns for the minority class and improve predictive performance.

Because SMOTE cannot process missing values, prior to implementing SMOTE we imputed values using CART in the mice package in R (van Buuren and Groothuis-Oudshoorn, 2011) for variables with less than 25% missing values. The variables with 25% or more missingness were dropped from the dataset. The resulting SMOTE-augmented dataset of independent variables included 1917 observations with 19 variables and 50% (n = 951) of observations with CFEI.

RESULTS

The primary task of machine learning models is to predict outcomes. Generally, models that predict outcomes more accurately are considered better models. The performance metrics indicate the RF model correctly classified the test data with 97.2% accuracy when using all 19 independent variables, which suggests strong predictive accuracy. This accuracy represents a significant improvement over simply predicting the modal outcome, which is 50% as a result of the SMOTE process of balancing the dataset. The confusion matrix shows that the model correctly classified 96.5% of non-targeted cases and 98.9% of targeted cases, which indicates slightly better predictive performance for targeted than non-targeted cases.

Variable Importance: RF Variable Importance Scores.

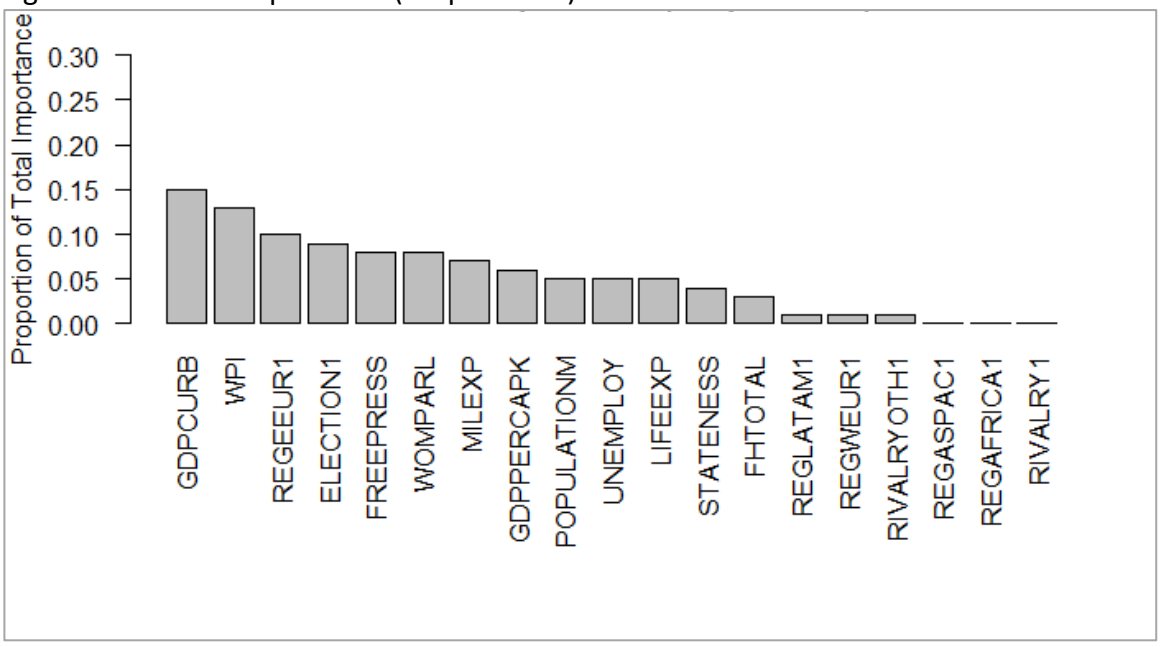
While interesting, the objective of this study is to identify factors related to the occurrence or not of CFEI, not simply to build the best predictive model. The RF algorithm can also estimate

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

independent variable importance using the Mean Decrease in Accuracy (Permutation Importance) method. In this method, after constructing the forest of trees, the model estimates the importance of each variable based on its contribution to improving predictive accuracy. The algorithm does this by randomizing the values of one variable in out-of-bag data to break its relationship with the dependent variable. It then checks how much the model's accuracy drops. The more the model's accuracy drops, the more important the variable is. The average drop in accuracy across all trees indicates the importance score for a variable.

Based on this method, Figure 1 indicates that current GDP (GDPCUR) is the most influential predictor, accounting for 15% of the total importance, followed by World Power Index score (WPI, 13%) and location or not in the Eastern European region (REGEEUR, 10%). Other variables with notable importance include temporal proximity to an election (ELECTION, 9%), press freedom (FREEPRESS, 8%), and percent women in parliament (WOMPARL, 8%). Together, these six variables account for more than 60% of the predictive improvement across the forest models.

Figure 1. Variable Importance (Proportional)



https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Lower-tier factors such as military expenditures as a percentage of GDP (MILEXP, 7%), GDP per capita (GDPPERCAPK, 6%), population (POPULATIONM, 5%), unemployment (UNEMPLOY, 5%), and life expectancy (LIFEEXP, 5%) highlight the role of economic strength, demographic size, and social development indicators. Variables such as governance capacity (STATENESS, 4%) and political liberty (FHTOTAL, 3%) contribute modestly, while the remaining regional indicators (REGLATAM, REGWEUR, REGASPAC, and REGAFRICA1) as well as ongoing major power (RIVALRY) and non-major power (RIVALRYOTH) rivalry add little predictive value to this model.

Overall, the RF variable importance scores suggest that the model's performance is most influenced by economic (GCPCUR) and geopolitical (WPI) strength as well as political context (REGEEUR and ELECTION) and political openness (FREEPRESS and WOMPARL).

Variable Importance: Logistic Regression.

RF modeling requires additional analyses to identify the strength and direction of relationships between the dependent and independent variables (Oka et al., 2025). Here we use bivariate logistic regression to identify the direction and strength of each independent variable's relationship with the dependent. Table 2 reports the variables by order of importance in terms of their RF importance score as discussed above. The table also reports the variables' rank by each bivariate model's Akaike Information Criterion (AIC). AIC is a measure of model quality that balances goodness of fit with model complexity. It is used to compare models to select the one that is likely to generalize best to new data. The best model has the lowest AIC, which in this case is WPI. The table also indicates the direction of relationship based on the regression model coefficient (+ indicates a positive relationship, and - indicates a negative relationship) and statistical significance of the estimated relationship between each independent variable and the dependent variable.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Table 2. Variable Importance Rankings: Univariate

	RF Analysis		Regression Analysis		
Variable	Impt Rank	Pct Total Impt	Impt Rank	AIC	Direction
GDPCUR	1	15	2	707.37	+ (*)
WPI	2	13	1	616.52	+ (*)
REGEEUR	3	10	12	777.46	+ (*)
ELECTION	4	9	3	715.24	+ (*)
FREEPRESS	5	8	19	799.68	-
WOMPARL	6	8	6	755.23	+ (*)
MILEXP	7	7	8	761.60	+ (*)
GDPPERCAPK	8	6	14	779.57	+ (*)
POPULATIONM	9	5	15	779.91	+ (*)
UNEMPLOY	10	5	18	798.78	+
LIFEEXP	11	5	4	723.02	+ (*)
STATENESS	12	4	5	745.56	+ (*)
FHTOTAL	13	3	16	785.84	+ (*)
REGLATAM	14	1	11	776.24	- (*)
REGWEUR	15	1	7	755.51	- (*)
RIVALRYOTH	16	1	17	785.94	+ (*)
REGASPAC	17	0	13	777.73	- (*)
REGAFRICA	18	0	9	769.39	- (*)
RIVALRY	19	0	10	769.82	+ (*)

* $p < 0.05$ in regression analyses

Based on the regression models, Table 2 indicates that 17 of the 19 relationships are statistically significant. The two variables that are not statistically related to the dependent variable are UNEMP and FREEPRESS. It also indicates that five of the 19 variables are negatively related to the occurrence of CFEI: REGWEUR, REGAFRICA, REGLATAM, REGASPAC, and FREEPRESS. The remaining variables are positively related to CFEI.

Raw AIC scores are not usefully interpretable; however, differences in AIC scores are. According to a widely used standard (Burnham and Anderson, 2004, 271), differences in AIC scores of two or less indicate models are essentially equivalent. That is, one model fits the data no better than the other. For example, the UNEMPLOY model (798.78) is no better than the FREEPRESS model (799.68). On the other hand, a model with an AIC score more than 10 points lower than another model is clearly better

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

according to this standard. For instance, the WPI model (616.52) is clearly better than all the other models; GDPCUR (707.37) is clearly better than 16 of the models; and ELECTION (715.24) and LIFEEXP (723.02) are clearly better than the 15 remaining models. Differences between four and seven points provide some evidence that the model with the lower score is better. In this case, for instance, POPULATIONM (779.91) is probably better than FHTOTAL (785.84) and RIVALRYOTH (785.94).

By these analyses, then, WPI (616.52 versus next lowest at 707.37) clearly stands out in the strength of its relationship with the occurrence of CFEI. This suggests that CFEI is more likely to occur in more geopolitically powerful countries. GDPCUR (707.37), ELECTION (715.24), and LIFEEXP (723.02) also stand apart from the remaining variables. These results suggest that CFEI is more likely to occur in more economically powerful countries, countries with temporally proximate elections, and countries whose citizens have longer life expectancies. Some analysts may also conclude that STATENESS (745.56) stands apart from the remaining variables. This suggests that CFEI is also more likely to occur in higher functioning states that can exert their authority and control across their entire territory and population.

Table 2 also permits the comparison of AIC-based and RF-based variable importance ranks. Both approaches indicate WPI and GDPCUR are the two most influential predictors, though their order is reversed between methods (WPI ranks first by AIC, while GDPCUR ranks first by RF). ELECTION also ranks highly in both models (third by AIC, fourth by RF), indicating consistent predictive value across approaches. Several variables show mid-level importance in both rankings, though their precise positions vary: WOMPARL, MILEXP, GDPPERCAPK, and POPULATIONM. In contrast, variables like FREEPRESS and UNEMPLOY rank lower by AIC but appear more influential in the random forest model, suggesting that non-linear or interaction effects may be present and better captured by RF variable importance scores. Conversely, regional indicators such as REGAFRICA, REGASPAC, and RIVALRY contribute minimally in both approaches, reinforcing their limited predictive role in the analysis.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

It should be noted that differences in variable importance between the two approaches may arise because AIC reflects model fit under a parametric, linear framework, while RF variable importance reflects predictive contribution in a non-parametric, interaction-aware model. These methods answer related but different questions: regression AIC focuses on model parsimony and explanatory power, whereas random forest importance focuses on predictive utility. Because the approaches vary, ranking similarities suggest more likely rankings.

Variable Importance: Model Reduction.

The previous variable importance analyses focused on individual variables to assess importance. Another way to identify the importance of variables follows the process suggested by Scime and Murray (2007) and Murray et al. (2009) in which variable importance is assessed using a multivariate approach. In this process, variables are removed one by one from the dataset starting, in this case, with the least important variable identified by RF variable importance score. Then a new model is trained and tested using the reduced dataset, and the accuracy of the new model built from the reduced dataset is compared to the previous model built using the larger dataset. When the models' accuracies are not statistically different, the dropped variable in the larger dataset is not important for predicting the dependent variable and can be removed from the list of important variables. When the accuracies are statistically different, the dropped variable should be considered for retention in the dataset.

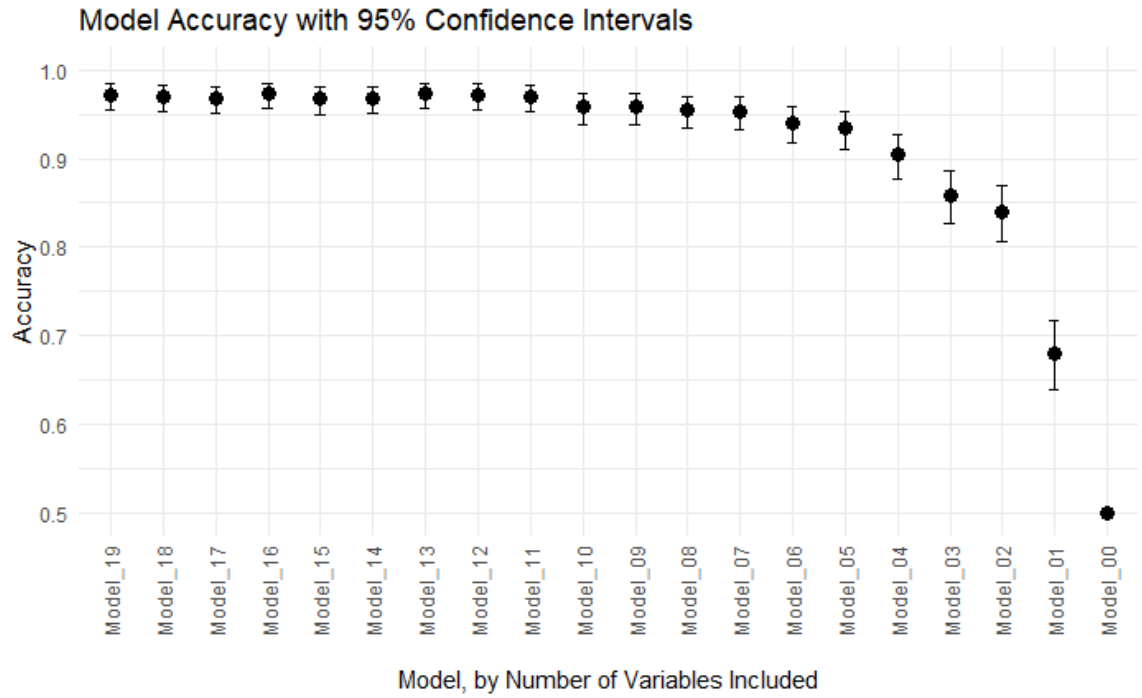
Figure 2 tracks the accuracy of the models starting on the left from the full dataset of 19 independent variables with a model accuracy of 97.2% to the accuracy of models with two (WPI and GDPCUR) and one (GDPCUR) independent variable with accuracies of 84.0% and 67.9%, respectively, on the right. The models are ordered by RF variable importance scores. As expected, the figure shows that accuracy drops as variables are removed from the dataset. McNemar's tests indicate the accuracies of Models 19 to 11 are statistically indistinguishable ($p \geq 0.05$). Model 10, which drops LIFEEXP, is

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

statistically less accurate ($p < 0.05$) than Model 11. This suggests that LIFEEXP has an important impact on model accuracy. Then, Models 10 to 5 are statistically indistinguishable in terms of accuracy. Model 4, which drops FREEPRESS, is statistically less accurate than Model 5. Finally, the accuracies of the remaining models are statistically different from each other. That is, Model 3, which drops ELECTION, is statistically less accurate than Model 4; Model 2, which drops REGEEUR, is statistically less accurate than Model 3; and Model 1, which drops WPI, is statistically less accurate than Model 2. Further, it is worth noting that the accuracy of Model 1 (67.9%) is statistically better than the accuracy of simply guessing the modal category (50.4%; $p < 0.001$), which is represented by Model_00 in Figure 2.

This analysis suggests, then, that the most parsimonious model, which retains the most predictive power with the fewest predictors, is Model 5: GDPCUR, WPI, REGEEUR, ELECTION, and FREEPRESS.

Figure 2.



https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Overall, the multivariate approach is consistent with the two univariate approaches indicating the small number of variables that have meaningful relationships with the occurrence or not of CFEI. GDPCUR, WPI, and ELECTION consistently rank among the top four most highly related variables with CFEI.

REGEEUR and FREEPRESS rank in the top five of the RF variable importance scores and are statistically related to multivariate predictive accuracy, but they rank lowly in regression variable importance. This could indicate there is an interactive component to their association with the dependent variable. This may especially be the case for FREEPRESS, which was not statistically significant in its bivariate regression model. WOMPARL and MILEXP consistently rank sixth to eighth in the univariate approaches, but they are not statistically related to predictive accuracy in the multivariate approach. In other words, the RF models are statistically as accurate without them as with them.

The relative performance of related variables also provides some insight into CFEI. GDPCUR, one of the top two variables, greatly outperforms the other two economic measures, GDPPERCAP and UNEMPLOY, which are mid- to low-tier performers. One interpretation is that economic size (GDPCUR) is more important than economic efficiency or performance (GDPPERCAP and UNEMPLOY). REGEEUR also stands out from the other regional variables (REGLATAM, REGWEUR, REGASPAC, and REGAFRICA). Not only does REGEEUR rank much higher in the RF univariate and multivariate variable importance analyses than the others, but it is also positively associated with the occurrence of CFEI while the others are negatively associated.

DISCUSSION

This study identifies several variables that tend to be related to CFEI. In particular, greater current GDP (GDPCUR) and geopolitical power (WPI) along with upcoming elections (ELECTION) are highly ranked as top predictors of CFEI in all three approaches to rating variable importance. Other

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

factors of possible interest are a greater proportion of women in parliament (WOMPARL), a greater proportion of military spending (MILEXP), location in the eastern European region (REGEEUR), and lesser press freedom (FREEPRESS). Having identified these factors, we can now use them to evaluate theories that may be used to explain the targets of CFEI.

Traditional international relations theory often focuses on power dynamics, that is, the relative power of the attacked versus attacking state. In broad terms, some theorists suggest that power equilibrium among states leads to peace (Waltz, 1979). Others argue that greater powers are more likely to attack lesser powers in an effort to maximize power (e.g., Mearsheimer, 2001). Some argue that weaker but rising states may attack dominant powers to challenge the status quo (Waltz 1979; Organski and Kugler 1980; Gilpin 1981). And still others suggest that weak states act more aggressively if they perceive even a temporary military, strategic, or political advantage (Lebow, 1984), such as when stronger states are distracted (Wolf, 1991). This study is consistent with the tendency for strong states to be targets, at least in terms of larger GDP, greater geopolitical power, and more spending on military resources. And there is other empirical evidence that this applies regarding cyberpower. For instance, Albert et al. (2024) finds that states that are most targeted by cyber-enabled influence campaigns on Facebook are wealthier on average and likely to spend more on defense (but see Hunter et al., 2021).

A lengthy discussion of balance of power theory is not appropriate here, but for the purposes of this study, one might argue that in cyberspace, lesser powered nation-states may use cyberpower as a way to balance the relative power of stronger actors. This has dramatic systemic impacts for theory development in the realm of cyberpower or in determining whether the paradigm of realism holds true in this domain. These results suggest that the basic theoretical findings (Waltz 1979; Organski and Kugler 1980; Gilpin 1981; Lebow, 1984; Wolf, 1991) hold steady in cyberspace: strong states are more likely to be targeted. This has implications for alliances, balancing, and what perhaps could be called cyber-bandwagoning or cyber-chainganging, where weaker states attach themselves to stronger states to

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

engage in cyberattacks against the dominant actor in the system or against more powerful actors, generally.

Reasons for this may be that weaker states think cyberoperations pose less risk of retaliation, so there is less of a deterrent, and/or that more powerful targets have less severe countermeasures in place. In other words, it is unlikely a state will strike kinetically as a second-strike against a cyber-affiliated or enhanced first strike, such as CFEI. Although there are examples of states responding from an attack in cyberspace with kinetic responses, the risk is minimal (Libicki 2020). This is in line with the literature of asymmetric conflict, of which many argue cyberpower fits within. Hagstrom (2025) argues that weaker actors often engage in asymmetric warfare, relying on political, social, and informational means to target stronger forces. This study suggests that CFEI may be an instance of asymmetric conflict. Much of the literature suggests cyberpower might be diffused across different actors relative to power, or that cyberpower aids the weaker to attack the stronger (Lindsay and Kello 2014; Siedler 2016; Hughes and Colarik 2016).

Regionality also plays a significant role. The results indicate that countries in the Eastern European region are much more likely to fall victim to CFEI than any other region. Overall, Valeriano and Maness (2014) contend that regionality, proximity to attacking state, and general regional affiliation are all attributes of targeted states. In a follow-up study, Maness et al. (2023, 78) note that the main targets of cyber operations in order of frequency have been the US, South Korea, Ukraine, India, and Israel, and note, “Increased intensity between rivals is the likely culprit behind this increase.” Standing out in this group is the US, which Valeriano and Maness (2014, 356) note is the global hegemon and the most connected major power, making it an attractive target for cyber aggression.

These results also suggest that regime type is not a significant factor. The Freedom House measure of political freedom (FHTOTAL) was never identified as a significant contributor to CFEI. Though Table 1 shows that targeted countries were more democratic than non-targeted countries, the

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

differences were not substantively large. It may just be that all the countries would be identified as democracies by these and other measures. Or it may be that an aggregation of some of the top predictors (e.g., ELECTION, FREEPRESS, and WOMPARL) capture the concept of greater democracy and account for variance that would have been accounted for by FHTOTAL in the absence of the other predictors.

This is important because it is contrary to previous research that suggests regime type does play a role in cyber conflict. Maness et al. (2023) report that democracies are targeted by cyber means more often than authoritarian regimes. Hunter et al. (2022) add that "Authoritarian states appear more likely to initiate cyberattacks, and more likely to target democracies, when compared with democratic states" (Hunter et al. 2022, 18; see also Hunter et al. 2024). On the other hand, Hunter et al. (2022) find that democracies are less likely to initiate cyberattacks compared to authoritarian regimes. But when they do initiate a cyber attack, they are significantly more likely to target authoritarian or at least less-democratic regimes (Hunter et al., 2024). These findings, then, also add insight into and raise more questions about the notion of cyber regime theory.

Overall, in some ways, the results of this study are consistent with Kallberg's (2016) notion of strategic cyberwar theory, which can be seen as a blend between cyberpower and cyber regime theories. Kallberg argues that cyberattacks work best when focused on bringing down or disrupting the institutions of a stable society, often by sowing and causing chaos within the targeted state. Our findings suggest that more powerful and economically stable countries are targeted with CFEI, supporting Kallberg. In the case of CFEI, the entire electoral system is the threat vector. This aligns with more traditional theories of international relations, including power transition theory and arguments regarding asymmetric conflict. While more research is needed, this study seems to demonstrate that cyber-operations, specifically CFEI, are a weapon of the weak, seeking to revise the status quo of the international system using asymmetric conflict.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Limitations and Future Research

This study is not without its limitations. Data quality, particularly imbalance in the dependent variable, is the primary concern. The machine learning algorithm requires balanced observations in the dependent variable to produce reliable random forest models. As such, we balanced the dataset using a statistical technique (SMOTE), which also required data to be imputed for several variables. While the data preprocessing improves the model's ability to identify patterns in the data, it may also introduce biases that could affect the generalizability of the results.

Replicating the study on a different dataset, potentially from another time period or a different set of countries, can confirm the robustness and generalizability of these findings. This approach helps ensure that the results are not specific to this particular dataset or due to any data anomalies. For instance, updating the dataset beyond 2020 and applying the same analytical framework could validate the predictive power of the model and identified factors in different contexts.

Employing a variety of statistical or machine learning techniques can also enhance the reliability of the findings. Different methods may have different sensitivities to the structure of the data and underlying assumptions. For example, while decision trees capture non-linear relationships and interactions among variables, other techniques like neural networks or ensemble models might uncover more complex patterns that decision trees might miss. Comparing results across these methods can provide a more comprehensive view of the data and help confirm key findings.

This study also raises questions about attackers. A future study could apply the quantitative approach here to attackers, which would provide a broader view of CFEI dynamics. This could include exploring who attackers are (e.g., state-sponsored, non-state actors), their motivations, and their resources. It could also include analyzing the tactics, techniques, and procedures used in CFEI campaigns as well as evaluating the impact of CFEI on election outcomes and public perception.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

CONCLUSION

Overall, the study is one of the first to quantitatively analyze states that are attacked, not attackers, using cyber-enabled foreign election interference. It uncovers some of the broad factors related to a country's vulnerability to CFEI, which in some ways can be situated in broader international relations theory. It offers a foundation for further investigation into the specific mechanisms through which these factors exert their influence. The findings may be particularly valuable for policymakers and cybersecurity experts who are tasked with enhancing the resilience of national electoral systems against such interference. Minimally, future research should continue to refine these models and explore the dynamic between cyber capabilities and traditional forms of influence, considering the evolving nature of cyber threats and the increasing sophistication of cyber operations. As cyber information warfare becomes a more prominent feature of international relations, understanding its impact on democratic institutions is crucial for maintaining the integrity of global political systems.

Regardless, the results suggest that more research beyond this exploratory study is warranted, particularly to build and test theory more rigorously. The study provides some early empirical evidence of the factors related to CFEI and possible theoretical context to help fit the empirics within the world of international security studies.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

APPENDIX A. List of CFEI Events

Target	Year	Attacker	Attack Vector
Armenia	2017	Russia	Information Warfare / Disinformation
Australia	2019	China	Hacking / Cyber Ops.
Brazil	2014	Russia	Information Warfare / Disinformation
Brazil	2018	Russia	Information Warfare / Disinformation
Bulgaria	2015	Russia	Hacking / Denial of Service
Colombia	2018	Russia	Hacking / Cyber Ops.
Czech Republic	2017	Russia	Hacking / Cyber Ops.
Czech Republic	2017	Russia	Information Warfare / Disinformation
Czech Republic	2018	Russia	Information Warfare / Disinformation
Finland	2019	Russia	Denial of Service Attack (DOS)
France	2017	Russia	Hacking / Cyber Ops.
France	2017	Russia	Hacking / Cyber Ops.
France	2017	Russia	Information Warfare / Disinformation
Germany	2017	Russia	Hacking / Cyber Ops.
Germany	2017	Russia	Information Warfare / Disinformation
Germany	2018	Russia	Information Warfare / Disinformation
Hong Kong	2016	China	Hacking / Cyber Ops.
Hong Kong	2018	China	Hacking / Cyber Ops.
Indonesia	2019	China	Hacking / Cyber Ops.
Indonesia	2019	Russia	Hacking / Cyber Ops.
Israel	2019	Iran	Hacking / Cyber Ops.
Italy	2016	Russia	Information Warfare / Disinformation
Italy	2018	Russia	Information Warfare / Disinformation
Italy	2018	Russia	Information Warfare / Disinformation
Italy	2018	Russia	Information Warfare / Disinformation
Lithuania	2018	Russia	Information Warfare / Disinformation
Madagascar	2018	Russia	Information Warfare / Disinformation
Malaysia	2018	China	Hacking / Cyber Ops.
Malta	2017	Russia	Hacking / Denial of Service
Montenegro	2016	Russia	Hacking / Denial of Service
Montenegro	2016	Russia	Information Warfare / Disinformation
Montenegro	2018	Russia	Hacking / Cyber Ops.
Mozambique	2019	Russia	Information Warfare / Disinformation
Netherlands	2016	Russia	Information Warfare / Disinformation
Netherlands	2017	Russia	Hacking / Cyber Ops.
Netherlands	2017	Russia	Information Warfare / Disinformation
North Macedonia	2018	UK	Influence Operations
North Macedonia	2018	Russia	Information Warfare / Disinformation

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

North Macedonia	2018	Russia	Information Warfare / Disinformation
North Macedonia	2018	Russia	Information Warfare / Disinformation
Norway	2017	Russia	Hacking / Cyber Ops.
Poland	2015	Russia	Information Warfare / Disinformation
Poland	2020	Russia	Information Warfare / Disinformation
Singapore	2017	China	Hacking / Cyber Ops.
Slovakia	2019	Russia	Information Warfare / Disinformation
South Africa	2019	Russia	Information Warfare / Disinformation
South Korea	2020	North Korea	Hacking / Cyber Ops.
Spain	2017	Russia	Information Warfare / Disinformation
Spain	2017	Russia	Information Warfare / Disinformation
Sweden	2018	Russia	Information Warfare / Disinformation
Taiwan	2018	China	Hacking / Cyber Ops.
Taiwan	2018	China	Information Warfare / Disinformation
Taiwan	2020	China	Information Warfare / Disinformation
Ukraine	2014	Russia	Hacking / Cyber Ops.
Ukraine	2014	Russia	Hacking / Cyber Ops.
Ukraine	2019	Russia	Hacking / Cyber Ops.
Ukraine	2019	Russia	Hacking / Denial of Service
Ukraine	2019	Russia	Information Warfare / Disinformation
Ukraine	2019	Russia	Information Warfare / Disinformation
Ukraine	2019	Russia	Denial of Service Attack (DOS)
United Kingdom	2014	Iran	Information Warfare / Disinformation
United Kingdom	2016	Iran	Information Warfare / Disinformation
United Kingdom	2016	Russia	Information Warfare / Disinformation
United Kingdom	2019	Russia	Information Warfare / Disinformation
United States	2016	Russia	Hacking / Cyber Ops.
United States	2016	Russia	Hacking / Cyber Ops.
United States	2016	Russia	Hacking / Cyber Ops.
United States	2016	Russia	Hacking / Cyber Ops.
United States	2016	Russia	Hacking / Cyber Ops.
United States	2016	Russia	Information Warfare / Disinformation
United States	2016	Russia	Information Warfare / Disinformation
United States	2018	Russia	Hacking / Cyber Ops.
United States	2018	Russia	Information Warfare / Disinformation
United States	2018	Russia	Information Warfare / Disinformation
United States	2018	Russia	Information Warfare / Disinformation
United States	2018	Russia	Information Warfare / Disinformation
United States	2018	Russia	Information Warfare / Disinformation
United States	2018	Russia	Information Warfare / Disinformation
United States	2018	Russia	Information Warfare / Disinformation

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

United States	2020	Iran	Hacking / Cyber Ops.
United States	2020	North Korea	Hacking / Cyber Ops.
United States	2020	Russia	Hacking / Cyber Ops.
United States	2020	Iran	Information Warfare / Disinformation
United States	2020	China	Hacking / Cyber Ops.
United States	2020	Russia	Information Warfare / Disinformation

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

APPENDIX B. Descriptions of Starting Variables

Variable	Description
AIREADY	AI Readiness from the Oxford Internet Institute.
AIVIB	Artificial Intelligence (AI) Vibrancy Index, representing an evaluation of each country's AI standing based on user preferences, key national indicators to guide policy decisions, and centers of AI excellence in both advanced and emerging economies. (Higher scores indicate that a country has higher levels of development and postures towards AI; lower scores indicate a country is less developed and not as well postured for AI solutions)
CINC	Composite Index of National Capability score, representing a country's estimated ability to wage war based on measures relevant to state power
COUNTRY	Indicates the individual country or region under analysis
ELECTVIOL1	Electoral Violence Index 1 score, representing the score based on a weighted ensemble of models (scores closer to 1.0 represent greater electoral violence; scores closer to 0.0 represent less risk of electoral violence)
ELECTVIOL2	Electoral Violence Index 2 score, representing the score based on the impact of social media and digital tools on elections (scores closer to 1.0 represent greater electoral violence; scores closer to 0.0 represent less risk of electoral violence)
FHSTATUS	Freedom House Status, which analyzes the electoral process, political pluralism and participation, the functioning of the government, freedom of expression and of belief, associational and organizational rights, the rule of law, and personal autonomy and individual rights in a country. Statuses are denoted as Free (F), Partially Free (PF), or Not Free (NF)
FHTOTAL	Freedom House Total Score, which represents the country's associated status as translated into a numerical indicator. (Numeric values indicate the following statuses: -1 to 29: Not Free; 30- 36: could be Not Free or Partially Free based on the aggregate of the analysis; 37-64: Partially Free; 65-72: could be Partially Free or Free based on the aggregate of the analysis; and, 73-100: Free)

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

FREEPRESS	Freedom of Press score, defined as the ability of journalists as individuals and collectives to select, produce, and disseminate news in the public interest independent of political, economic, legal, and social interference and in the absence of threats to their physical and mental safety(Scoring Methodology: For years 2002-2012, higher scores indicate less press freedom. For years 2013-present, higher scores indicate more freedom.)
GDPCUR	Current GDP of a country, defined as the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. Data are in current U.S. dollars.
GDPGROW	Current GDP of a country, defined as the sum of gross value added by all resident producers in the economy plus any product taxes and minus any subsidies not included in the value of the products. Data are in current U.S. dollars.
GDPPERCAP	Gross Domestic Product (GDP) per capita is calculated by GDP divided by midyear population. Data are in constant 2015 U.S. dollars.
GII	Global Innovation Index (GII) ranks the innovation performance of a country and its economy to track what country is leading in comparison to each other. (Higher scores indicate higher levels of innovation and performance)
GINI	Gini Index; measures the extent to which the distribution of income (or, in some cases, consumption expenditure) among individuals or households within an economy deviates from a perfectly equal distribution. (A Gini index of 0 represents perfect equality, while an index of 100 implies perfect inequality)
GMI	Global Militarization Index, expressed as a score which compares a country's overall military expenditure with its GDP and its health expenditure, as well as the number of heavy weapons in a country. (Higher GMI scores indicate a much higher rate of militarization, whereas lower GMI scores indicate weak militarization in a country.
GLOBINFINDX	Global Influence Index, representing the influence of both the U.S. and China across global economic, political, and security spectrums to track whether countries ultimately lean towards US influence, Chinese Influence, or neutrality. Index scoring is as follows: China Aligned (-100 to -10); Swing States/ Neutral States (-10 to +10); US Aligned (+10 to +100) 00.00

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

GOVAIREADY	Government AI Readiness Index, representing how ready a government is to integrate AI into public service delivery. (For year 2019, values are measured 0.00 to 10.00; for years 2020-2024, values are measured 0.00 to 100.00. For all years, higher scores indicate higher readiness posture towards AI)
LIFEEXP	Life expectancy at birth indicates the number of years a newborn infant would live if prevailing patterns of mortality at the time of its birth were to stay the same throughout its life
LITERACY	Represents the total literacy rate of all adults (aged 15 and older) in a country; Literacy is defined as an ability to both read and write with understanding a short simple statement about everyday life
MILEXP	Military Expenditure expressed as a percentage of a given country's GDP. Military Expenditure includes all current and capital expenditures on the armed forces, including peacekeeping forces; defense ministries and other government agencies engaged in defense projects; paramilitary forces, if these are judged to be trained and equipped for military operations; and military space activities.
POLITY2	Polity2 is a Revised Combined Polity Score; This variable is a modified version of the POLITY variable added in order to facilitate the use of the POLITY regime measure in time-series analyses. It modifies the combined annual POLITY score by applying a simple treatment, or ""fix," to convert instances of "standardized authority scores" (i.e., -66, -77, and -88) to conventional polity scores (i.e., within the range, -10 to +10). The values have been converted according to the following rule set: -66 Cases of foreign "interruption" are treated as "system missing." -77 Cases of "interregnum," or anarchy, are converted to a "neutral". Polity score of "0." -88 Cases of "transition" are prorated across the span of the transition
POPDEN	Population Density, calculated by the midyear population of a country divided by that country's land area in square kilometers.
POPULATION	Represents the total value of an entire population of a given country; Population is based on the de facto definition of population, which counts all residents regardless of legal status or citizenship

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

POPURBPCT	Represents the urban population as a percentage of the total population in a given country; Urban population refers to people living in urban areas, as defined by national statistical offices
REGAFRICA	indicator variable for Africa region
REGASPAC	indicator variable for Asia-Pacific region
REGEEUR	indicator variable for E European region
REGLATAM	indicator variable for Latin America/Caribbean region
REGWEUR	indicator variable for W European region
RESDEVT	Research and Development (R&D) expressed as a percent of GDP. R&D covers basic research, applied research, and experimental development
STATENESS	Stateness Index, expressed as a score of 0.0 to 1.0, indicating the extent to which a state can exercise its authority throughout its entire territory and the people living within it. Stateness indices are as follows: High functioning State (1 – 0.7, all dimensional scores above 0.7); Moderate functioning State (<0.7 – 0.5, one or more dimensional scores below 0.7 and all above 0.5); Defective State (<0.5 – 0.3, one or more dimensional scores below 0.5 and all above 0.3); Profound defective State (<0.3 – 0.1, one or more dimensional scores below 0.3 and all above 0.1); Collapsed State (< 0.1, one or more dimensional scores below 0.1)
TARGETED	Indicator variable coded 1 when a country-year included a CFEI and 0 otherwise. Dependent variable.
UNEMPLOY	Represents total unemployment rate for a given year, as a percentage of the total labor force of the country
UNREGION	Indicates the UN-recognized global region category for which an individual country belongs to
UNSECCOUN	An indicator variable coded 1 when the country was a permanent member of the UN Security Council and 0 otherwise.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

WOMPARL	Women Held Seats in national parliaments, expressed as a percentage of total parliamentary seats in a single or lower chamber
WPI	World Power Index (WPI) Score, which measures a country's national power as evaluated on material, semi-material, and immaterial capacities to define a state's multifaceted and dynamic power. Index scores closer to 1.0 indicate the highest level of national power; Index scores closer to 0.0 indicate less national power.
YEAR	Indicates the year for which the applicable data was collected

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

REFERENCES

Albert, Craig Douglas, Lance Y. Hunter, Samantha Mullaney, and Meagan Mays. 2024. “Analyzing Influence Operations on Facebook: An Exploratory Study.” *Digital War* 5 (3): 190–200.

Asevameh, Innocent Oshoke, Oladipupo Michael Dopamu, and Joseph Seun Adesiyan. 2024. “Election Infrastructure Security: A Review of Vulnerability and Impact on the US Economic Reputation.” *World Journal of Advanced Engineering Technology and Sciences* 12: 233–44.

Attatfa, Amel, Karen Renaud, and Stefano De Paoli. 2020. “Cyber Diplomacy: A Systematic Literature Review.” *Procedia Computer Science* 176: 60–69.

Brantly, Aaron, and Max Smeets. 2020. “Military Operations in Cyberspace.” In *Handbook of Military Sciences*, 1–16.

Burnham, Kenneth P., and David R. Anderson. 2004. “Multimodel Inference: Understanding AIC and BIC in Model Selection.” *Sociological Methods & Research* 33 (2): 261–304.

Dunn-Cavelty, Myriam. 2014. “Breaking the Cyber-Security Dilemma: Aligning Security Needs and Removing Vulnerabilities.” *Science and Engineering Ethics* 20 (3): 701–15.

Freedom House. 2021. *Freedom in the World 2020*. Lanham, MD: Rowman & Littlefield.

Gilpin, Robert. 1981. *War and Change in World Politics*. Cambridge: Cambridge University Press.

Gorwa, Robert, and Max Smeets. 2019. “Cyber Conflict in Political Science: A Review of Methods and Literature.” *OSF Preprints*.

Hagstrom, Jacob. 2025. *Asymmetric Warfare: Politics and Cultures of Violence in the Modern Era*. Cambridge: Cambridge University Press.

Hansen, Isabella, and Darren J. Lim. 2019. “Doxing Democracy: Influencing Elections via Cyber Voter Interference.” *Contemporary Politics* 25 (2): 150–71.

Hanson, Fergus, Emilia Currey, and Tracy Beattie. 2020. “Cyber-Enabled Foreign Interference in Elections and Referendums.” *Australian Strategic Policy Institute Report* 41: 1–63.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Hanson, Fergus, Sarah O'Conner, Mali Walker, and Luke Courtois. 2019. "Hacking Democracies: Cataloguing Cyber-Enabled Attacks on Elections." *Australian Strategic Policy Institute Report* 16: 1–30.

Hughes, Daniel, and Andrew M. Colarik. 2016. "Predicting the Proliferation of Cyber Weapons into Small States." *Joint Force Quarterly* 83 (4): 19–26.

Hunter, Lance Y., Craig D. Albert, and Eric Garrett. 2021. "Factors That Motivate State-Sponsored Cyberattacks." *The Cyber Defense Review* 6 (2): 111–28.

Hunter, Lance Y., Craig D. Albert, Eric Garrett, and Josh Rutland. 2022. "Democracy and Cyberconflict: How Regime Type Affects State-Sponsored Cyberattacks." *Journal of Cyber Policy* 7 (1): 72–94.

Hunter, Lance Y., Craig Douglas Albert, Steven Cauthron, and Rose Antilla. 2024. "When Democracies Attack: Examining the Offensive Strategies of Democracies in Cyberspace." *Global Perspectives* 5 (1): 127548.

Kallberg, Jan. 2016. "Strategic Cyberwar Theory: A Foundation for Designing Decisive Strategic Cyberoperations." *The Cyber Defense Review* 1 (1).

Keitner, Chimène. 2020. "Foreign Election Interference and International Law." *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3599586.

Kuhn, Max. 2008. "Building Predictive Models in R Using the caret Package." *Journal of Statistical Software* 28 (5): 1–26.

Lebow, Richard Ned. 1984. "Windows of Opportunity: Do States Jump through Them?" *International Security* 9 (1): 147–86.

Libicki, Martin C. 2020. "Correlations between Cyberspace Attacks and Kinetic Attacks." In *Proceedings of the 2020 12th International Conference on Cyber Conflict (CyCon)*, vol. 1300, 199–213. IEEE.

Lindsay, Jon R., and Lucas Kello. 2014. "Correspondence: A Cyber Disagreement." *International Security* 39 (2): 181–92.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Maness, Ryan C., Brandon Valeriano, Kathryn Hedgecock, Jose M. Macias, and Benjamin Jensen. 2023. "Expanding the Dyadic Cyber Incident and Campaign Dataset (DCID)." *The Cyber Defense Review* 8 (2): 65–90.

Manwaring, Rob, and Josh Holloway. 2023. "Resilience to Cyber-Enabled Foreign Interference: Citizen Understanding and Threat Perceptions." *Defence Studies* 23 (2): 334–57.

Marshall Palmer, J., and Alex Wilner. 2024. "Deterrence and Foreign Election Intervention: Securing Democracy through Punishment, Denial, and Delegitimization." *Journal of Global Security Studies* 9 (2).

Mearsheimer, John J. 2001. *The Tragedy of Great Power Politics*. New York: W. W. Norton.

Murray, Gregg R., Chris Riley, and Anthony Scime. 2009. "Pre-Election Polling: Identifying Likely Voters Using Iterative Expert Data Mining." *Public Opinion Quarterly* 73 (1): 159–71.

O'Connor, Sarah, Fergus Hanson, Emilia Currey, and Tracy Beattie. 2020. *Cyber-Enabled Foreign Interference in Elections and Referendums*. Vol. 28. Canberra: Australian Strategic Policy Institute.

Ohlin, Jens David. 2020. *Election Interference: International Law and the Future of Democracy*. Cambridge: Cambridge University Press.

Ohlin, Jens David, and Duncan B. Hollis. 2021. *Defending Democracies: Combating Foreign Election Interference in a Digital Age*. Oxford: Oxford University Press.

Oka, Souichi, Takuma Yamazaki, and Yoshiyasu Takefuji. 2025. "Complementary Statistical Approaches for Interpreting Machine Learning Feature Importance in Osteoporosis Risk." *Computers in Biology and Medicine* 196: 110710.

Organski, Abramo F. K., and Jacek Kugler. 1980. *The War Ledger*. Chicago: University of Chicago Press.

Schia, Niels Nagelhus, and Lars Gjesvik. 2020. "Hacking Democracy: Managing Influence Campaigns and Disinformation in the Digital Age." *Journal of Cyber Policy* 5 (3): 413–28.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Scime, Anthony, and Gregg R. Murray. 2007. “Vote Prediction by Iterative Domain Knowledge and Attribute Elimination.” *International Journal of Business Intelligence and Data Mining* 2 (2): 160–76.

Shackelford, Scott J., Anjanette Raymond, Abbey Stemler, and Cyanne Loyle. 2020. “Defending Democracy: Taking Stock of the Global Fight against Digital Repression, Disinformation, and Election Insecurity.” *SSRN Electronic Journal*.

Shorey, Samantha, and Philip N. Howard. 2016. “Automation, Big Data, and Politics: A Research Review.” *International Journal of Communication*: 5032–55.

Siedler, Ragnhild Endresen. 2016. “Hard Power in Cyberspace: CNA as a Political Means.” In *Proceedings of the 2016 8th International Conference on Cyber Conflict (CyCon)*, 23–36. IEEE.

Siriseriwan, W. 2024. “smotefamily: A Collection of Oversampling Techniques for Class Imbalance Problem Based on SMOTE.” R package version 1.4.0.

Slayton, Rebecca. 2017. “What Is the Cyber Offense-Defense Balance? Conceptions, Causes, and Assessment.” *International Security* 41 (3): 72–109.

Stedmon, Nicholas. 2020. “The Impact of Cyber Security Threats on the 2020 US Elections.” *arXiv Preprint*.

Tucker, Joshua, Andrew Guess, Pablo Barberá, Cristian Vaccari, Alexandra Siegel, Sergey Sanovich, Denis Stukal, and Brendan Nyhan. 2018. “Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature.” *SSRN Electronic Journal*.

Valeriano, Brandon, and Ryan C. Maness. 2014. “The Dynamics of Cyber Conflict between Rival Antagonists, 2001–11.” *Journal of Peace Research* 51 (3): 347–60.

Van Buuren, Stef, and Karin Groothuis-Oudshoorn. 2011. “Mice: Multivariate Imputation by Chained Equations in R.” *Journal of Statistical Software* 45 (3): 1–67.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0

Vićić, Jelena, and Erik Gartzke. 2024. “Cyber-Enabled Influence Operations as a ‘Center of Gravity’ in Cyberconflict: The Example of Russian Foreign Interference in the 2016 US Federal Election.” *Journal of Peace Research* 61 (1): 10–27.

Waltz, Kenneth N. 1979. *Theory of International Politics*. New York: Random House.

Whyte, Christopher. 2020. “Cyber Conflict or Democracy ‘Hacked’? How Cyber Operations Enhance Information Warfare.” *Journal of Cybersecurity* 6 (1).

Wolf, Barry. 1991. *When the Weak Attack the Strong: Failures of Deterrence*. RAND Corporation.

https://doi.org/10.33774/apsa-2026-wlcqm **ORCID:** https://orcid.org/0000-0003-3225-9386 Content not peer-reviewed by APSA. **License:** CC BY-NC-SA 4.0