Utah State University

DigitalCommons@USU

All Graduate Theses and Dissertations, Fall 2023 to Present

Graduate Studies

5-2024

Public Cyberattack Attribution and Domestic Political Considerations: An Analysis of State Decision Making

Ella M. Devey
Utah State University, ella.devey@usu.edu

Follow this and additional works at: https://digitalcommons.usu.edu/etd2023

Part of the Political Science Commons

Recommended Citation

Devey, Ella M., "Public Cyberattack Attribution and Domestic Political Considerations: An Analysis of State Decision Making" (2024). *All Graduate Theses and Dissertations, Fall 2023 to Present*. 193.
https://digitalcommons.usu.edu/etd2023/193

This Thesis is brought to you for free and open access by the Graduate Studies at DigitalCommons@USU. It has been accepted for inclusion in All Graduate Theses and Dissertations, Fall 2023 to Present by an authorized administrator of DigitalCommons@USU. For more information, please contact digitalcommons@usu.edu.

UtahStateUniversity
MERRILL-CAZIER LIBRARY

PUBLIC CYBERATTACK ATTRIBUTION AND DOMESTIC POLITICAL CONSIDERATIONS: AN ANALYSIS OF STATE DECISION MAKING

by

Ella M. Devey

A thesis submitted in partial fulfillment
of the requirements for the degree

of

MASTER OF SCIENCE

in

Political Science

Approved:

Austin Knuppe, Ph.D.
Committee Chair

Colin Flint, Ph.D.
Committee Member

David Winberg, M.S.
Committee Member

D. Richard Cutler, Ph.D.
Vice Provost for Graduate Studies

UTAH STATE UNIVERSITY
Logan, Utah

2024

Copyright © Ella Devey 2024

All Rights Reserved

ABSTRACT

Public Cyberattack Attribution and Domestic Political Considerations: An Analysis of State Decision Making

by

Ella M. Devey, Master of Science

Utah State University, 2024

Major Professor: Dr. Austin Knuppe
Department: Political Science

Cyberattacks are an increasingly utilized weapon of international conflict by state- and non-state actors. Following a cyberattack on a public or private sector target, the government of a targeted state may choose to publicly attribute the perpetrators of the cyberattack. Alternatively, they may be unable to identify the perpetrators or choose to keep their attribution private. It is known that conflict strategy and forensic capability influence a state’s public attribution behavior following a cyberattack, but might domestic political factors also contribute to attribution decisions among government actors?

Consistent with existing theories of International Relations, the approaches of government actors during cyber conflict may be in part due to their own regime type, the regime type of their opponent, and the perceptions of their domestic audiences and press. This study finds a positive association between the odds of public cyberattack attribution among states with greater degrees of press freedom as well as a decreased odds of public attribution when both the target and the suspected initiator are democratic. Understanding the complexity of state attribution choices will inform international cyber conflict and war perceptions and aid in the anticipation of conflict and war escalation.

(55 pages)

PUBLIC ABSTRACT

Public Cyberattack Attribution and Domestic Political Considerations: An Analysis of State Decision Making

Ella Devey

When a country is targeted with a cyberattack, what compels its government to publicly attribute the perpetrators of the attack rather than keep their attribution private? Cyberattacks are an increasingly utilized weapon of international conflict by governments, groups, and individuals. Following a cyberattack, the target of the attack may investigate the origin of the attack and may choose to share their findings with the public; alternatively, they may choose not to publicly share their findings.

While we know that forensic capabilities and international political factors contribute to the decision of governments to make public cyberattack attribution, domestic political circumstances may also inform this choice. This study finds a positive association between the odds of public cyberattack attribution among countries with greater degrees of press freedom as well as a decreased odds of public attribution when both the target and the suspected initiator are democracies. Understanding the complexity of government attribution choices will inform international cyber conflict and war perceptions and aid in the anticipation of conflict and war escalation.

ACKNOWLEDGMENTS

I would like to thank my committee chair Austin Knuppe and committee members Colin Flint and David Winberg for their support through my entire thesis process. From thinking through ideas for a proposal to the analysis and writing of my findings, I am immensely grateful for their expertise, patience, and encouragement. I am also grateful for all of the other faculty at USU that have taught and inspired me throughout my undergraduate and graduate studies.

I would also like to thank my wonderful family for supporting me during my education, as well as my friends and colleagues that have been there to encourage me every step of this project. I couldn’t have gotten to this place without the terrific people in my life to cheer me on.

Ella Devey

CONTENTS

Page

LIST OF TABLES

Page

LIST OF FIGURES

Page

INTRODUCTION

The use of cyberattacks as a means of fighting international conflict has garnered wide attention, fear, and speculation since the adoption of the internet across the world. Events such as the 2010 Stuxnet attack on an Iranian nuclear facility and the 2017 WannaCry global ransomware attack have highlighted cyber conflict as a new and effective method of interstate fighting. Unlike conventional warfare, cyberattacks can be conducted across the world, anonymously, and sometimes without detection.

In the aftermath of a cyberattack, the targeted entity may attempt to investigate and identify the perpetrators, motivations, and tactics behind the attack. Investigations are difficult, and even when the perpetrator can be identified, a government may choose not to publicly attribute the attack for strategic reasons. Understanding the circumstances surrounding cyberattack attribution is important because attribution can lead to conflict escalation, even unintended escalation and escalation resulting from false attribution made on unclear evidence (Acton 2020). Public attribution can shape public perceptions of global conflict, especially when global communication can occur quickly and freely. *Under what conditions, then, do government actors publicly attribute the perpetrators of cyberattacks?*

This study offers a series of risks and benefits that a government may weigh in the decision to publicly attribute a cyberattack, including the consideration of domestic audiences, which have largely been unexplored in the cyber context. The statistical models in this study show a positive association between a targeted state’s degree of press freedom and their odds of cyberattack attribution, as well as an increase in the odds of public attribution among targeted democracies when the initiator is a non-democracy.

In this paper, I first evaluate existing literature on cyber conflict and cyberattack attribution. The following sections detail the data and statistical methods used to analyze patterns of public cyberattack attribution. Three subsequent case studies explore the dimensions of attribution decision-making for state actors, including the factors found in the empirical analysis of this study. Together, these findings demonstrate the complexity of state cyberattack attribution decisions, offering clues for the future of cyber conflict and escalation.

LITERATURE REVIEW

The Emergence of Cyber Conflict

Cyber conflict research is relatively new but has evolved since its inception. Scholars in the 1990s cautioned during the widespread adoption of the internet that cyberattacks could become a critical means of warfighting, and that with no policies or treaties to mitigate damage as more systems became digital, great harm was inevitable (Nitzberg 1999; Hinde 1998; Rathmell 1999). Such pieces explore the unique anonymity offered by the internet and the novelty of the ability to engage in warfare from across the world with only keyboard strokes. A particularly ominous article entitled "Cyberwar is Coming!" (Arquilla and Ronfeldt 1993) warned that "cyberwar may be to the 21st Century what blitzkrieg was to the 20th."

While fears of cyberwarfare reaching a "blitzkrieg" magnitude have not yet come to fruition, high-profile cyberattacks have highlighted the ability of cyberattacks to inflict acute levels of physical harm on people and systems (McConnell 2009; Sampanis et al. 2023). Among the most infamous cyberattacks in history, the 2010 Stuxnet cyberattack damaged hundreds of centrifuges at the Iranian nuclear facility near Natanz and is suspected to have been initiated by Israel and the United States. Stuxnet spurred a new generation of cyber conflict research with varying degrees of alarm at the new-found potential of cyber weapons, making cyber conflict a forefront of academic and policy thinking (Farwell 2011; Rid 2011).

States have since had to reconcile the cyber domain as a new arena of fighting conflict within and across borders, as cyber conflict is often politically motivated but differs from conventional conflict in several important ways. One challenge is the distinction between war and conflict in the cyber arena; some cyberattacks happen as an extension of an existing war, and others are precursors or tools to war and conflict (Demchak 2010). Unlike conventional warfare, it is possible to engage in hacking from across the world with no need for proximity to the target (Deeks 2013). The attacker can choose to make their identity known or attempt to conceal it. In contrast, it is essentially impossible to conduct conventional conflict while concealing one’s identity (Reich et al. 2010).

Cyber conflict also differs from conventional conflict in that it can be conducted by anyone, including states, proxy groups working on behalf of a states, independent groups, and individuals. The lines between these categories are often unclear (Czosseck 2013). Motivations for initiating a cyberattack may include political gain, financial incentives, boredom, or pride (Paganini 2022; Stanton 2023). For non-state actors and those who become interested in state affiliated hacking, the cultural components of online hacking communities can be appealing in that they provide comradery and a feeling of achievement (Thackray 2018). Among state actors, most cyber conflict can be classified as attempts at subversion. Maschmeyer (2022) argues that cyber conflict should be viewed as an extended opportunity to erode targets rather than a type of warfare in itself. Schneider et al. (2022) similarly argue that cyber operations are a complement to diplomacy and narrative shaping prior to war and a tool in war once one has started.

Cyberattack Attribution

Among the complex dimensions of cyber conflict is that of cyberattack attribution. Literature specifically exploring the dimensions of cyberattack attribution is developing and largely qualitative due to the lack of datasets available to conduct large statistical studies. On initial observation of the issue of cyberattack attribution, one may assume that the technical capacity of the target entity will determine whether the target will publicly attribute the attack. Cyberattack forensics requires a high degree of technical and investigative expertise based on the type of attack and can limit attribution abilities (Boebert 2010; Mueller et al. 2019).

Identifying the perpetrator of a cyberattack is often costly for the investigative body, requiring finances, expertise, and time. In many cases, the investigative process requires the expertise of network analysts, cybersecurity analysts and engineers, private sector professionals, witnesses, and geopolitical analysts. The technical side of the forensic process includes analyses of code modularity, keystrokes, language use, attack sophistication, and device identifiers (Boerbert 2010; Rid and Buchanan 2014; Goel 2020). In particularly difficult cases, the involved bodies may decide that the money and personnel needed for attribution are better used elsewhere.

Cyberattack attribution is when an investigative entity deduces the origin and perpetrator of a cyberattack. Attribution can be made under varying degrees of certainty that the accusation is correct, as the attributor is often not entirely certain who initiated the attack. Even high-profile and thoroughly studied attacks, such as Stuxnet in 2010 and the Democratic National Committee attack in 2015, face questions of exact attack origins (Schulzke 2018). There is a risk under any level of attribution confidence that biases and goals may lead a government to falsely accuse an adversary of an attack when evidence is uncertain (Rid and Buchanan 2014).

Emerging literature suggests that attributing a cyberattack can signal intentions and knowledge, making it a strategic and political event. In an analysis and series of case studies, Tran (2018) suggests that the technical challenges of attribution are overstated and that strategic challenges are more influential than they may seem, using major cyberattack case studies to demonstrate the strategic considerations that overshadowed technical attribution processes. Rid and Buchanan (2014) describe the attribution of cyberattacks as “a function of what is at stake politically”: when an attack happens, pointing blame is a difficult and nuanced process, but can bolster collective defenses and enhance the appearance of credibility for the attributer. This is in congruence with the argument of Libicki (2009) who contends that a state’s foreign policy stances also influence cyberattack attribution patterns. Egloff and Smeets (2023) and Egloff (2020) theorize that attribution in cyberspace is a result of governments’ desires to shape the normative and political environments of global cyber conflict and that the goals of attribution for government can be enabled and constrained through geopolitics, intelligence, attack severity, and cooperative action.

Edwards et al. (2017) explore several considerations that a state may weigh when deciding whether to make a public attribution, including technological capacity symmetry and opponent perceptions. Their novel contribution, however, is to suggest that the lack of an appropriate response may influence the decision to make a public attribution. When a target country has no equivalent target to attack in the initiating country, their only options are to ignore the attack, respond disproportionately in the cyber domain, or retaliate in a non-cyber domain. Using a game theoretic model, they predict that states will avoid public attribution without an appropriate attack response or posture, particularly when subject to public criticism.

Rid and Buchanan (2014) argue that when a government entity releases more details about a cyberattack, the credibility of the government and the information about the attack increases. Additionally, the tactics, techniques, and procedures (TTPs) of an attack can be selectively revealed to control the narrative on the behavior of the threat actor (Egloff and Smeets 2023). Libicki (2009) proposes that it is within a government's best interest to be fully transparent in disclosing and attributing attacks to best control the spread of information about the attack and prevent unfounded or harmful speculation among the media and public.

Law organizations attempt to create frameworks for governments to follow in assigning blame to other countries for cyberattacks. Some suggest that attribution is more effective when made by both public and private actors, and that countries should follow a uniform legal standard of evidence for attribution (Eichensehr 2020). Additionally, legal frameworks may be used in conjunction with technical frameworks to determine the sufficient degree of certainty to make a public attack attribution (Tran 2018).

Cyberattack attribution can reduce plausible deniability for the attacker. Plausible deniability may motivate cyberattacks, particularly for proxy attacks supported but not conducted by government actors. The initiator can claim that they had nothing to do with the attack to avoid retaliatory action from the target. However, when a targeted government attributes an attack, the attack becomes less plausibly deniable for the initiator and future attacks may be deterred (Canfil 2022; Clement 2012).

These works demonstrate the technical and political challenges that have evolved with cyber conflict since its inception. While cyber conflict has not yet reached the magnitude feared by early scholars, cyberattacks have at some point interrupted all sectors of modern life. Cyberattacks attribution requires time, expertise, and money from the investigative body. Beyond technical capacity, however, signaling and other strategic interests may affect a government or private company’s choice to make public cyberattack attributions. Cyber research will expand as more case studies and data become available for study.

THEORY AND HYPOTEHSES

I argue that domestic political conditions--including regime types and domestic press freedom-- contribute to a government’s decisions to publicly attribute cyberattacks in conjunction with technical capacity and international politics. The public can become aware of cyber incidents by several means, including media releases, news outlets, social media, private sector announcements, and government announcements. Some attributions are made in private settings, typically between governments; other attributions, however, are made in the public sphere for all to see. What conditions, then, influence a government to publicly blame a perpetrator for a cyberattack?

Public Attribution Risks and Benefits

We may conceptualize this decision-making process through a series of potential risks and benefits. A government may benefit from the public attribution of an incident because it can improve the appearance of competence in the pursuit of national security threats and improve its image as a legitimate political authority, as well as allow it to preemptively shape the account of the attack in a way that improves its appearance of competence (Libicki 2009; Egloff and Smeets 2023). A government may be responsible for informing citizens of cyber incidents, especially in cases where an incident caused a high degree of damage. Additionally, public attribution may cause an attacker to cease their operation or serve as a warning against future operations (Egloff 2020).

Conversely, it may be more beneficial for a government to withhold public attribution as a matter of strategy. Public attribution may be viewed as an act of aggression by the suspected initiator, it may interfere with an investigation or endanger those involved in the investigation (Rid and Buchannan 2014). The government of the targeted country may lack an appropriate response to the attack (Edwards et al. 2017). When the public becomes aware of a cyber incident and its perpetrator, a government may face pressure from its public to take further retaliatory measures, which can become an issue if escalatory retaliation is against the strategic interests of the targeted state (Libicki 2009). Additionally, the attribution may be wrong, risking escalation if one state falsely accuses another of an attack (Eichensehr 2020).

A further risk is that future attackers may look back to publicly known cases of cyberattacks and learn from the initiator's tactics, techniques, and procedures, as well as learn from how the initiator was caught and how the target approached a response (Edwards et al. 2017). Public attribution may expose vulnerabilities in the target's systems; therefore, it may be within a target's interest to withhold this information to prevent future attackers from copying the attack (Libicki 2009). If this information is kept private, future attackers may be less effective in their planning.

The risk of exposing sensitive information during government attribution may be of additional concern if the target is in the private sector. For example, following the cyberattack by North Korean hackers on Sony Pictures following the release of a film depicting an assassination plot of Kim Jong Un, US officials promptly assigned blame for the incident to North Korea, citing the political relevance of the hack and its threat to US expression freedoms (Perlroth 2014; Peterson 2014). By conducting their own investigations and releases, however, government officials may have exposed company vulnerabilities that Sony Pictures would not have revealed themselves.

Given these considerations, this research will test several measures of domestic audience behavior and preference against instances of cyberattack attribution. These factors have been studied only minimally in the literature on cyberattack attribution despite their existing role in theories of International Relations.

Regime Type Dyads as Correlates of Public Attribution

The regime types of the initiating and targeted countries may impact public attribution decisions. The "democratic peace" predicts that democracies are less likely to engage in war with other democracies, as compared to autocracies. While this pattern is apparent, the causal mechanisms behind it are highly contested (Reiter 2017). Explanatory theories fall into normative, structural, and cultural categories. Normative explanations posit that citizens of democracies are intrinsically opposed to violent conflict, causing their governments to resolve conflict through peaceful or diplomatic means before escalating to violent conflict (Owen 1994; Maoz and Russett 1993; Tomz and Weeks 2013). Cultural explanations hypothesize that cultural norms typically shared across democracies influences conflict more than regime type itself (Goldcamp 2001). Structural arguments propose that the political structures found in democracies, such as size of decision-making bodies, creates incentives for leaders to avoid war between democracies (de Mesquita et al. 2014; LeVeck and Narang 2017; Maoz and Russett 1993; Adiputera 2017).

Other scholars argue that it is not democracy, but other factors associated with democracy that cause the pattern of democratic peace (Rosato 2003). Some, such as Gartzke (2007) and Mousseau (2013), have argued that free-market capitalism, which often accompanies democratic political systems, is a better explanation for the lack of war. Perhaps the mutual economic ramifications of war prevent countries that are economically interdependent from fighting one another, causing them to opt for other forms of conflict resolution.

As noted in the previous section, cyber conflict differs from conventional war in many ways, including that it is less visible, more anonymous, and typically less harmful than conventional military operations. Despite the differences between cyber and conventional conflict, might the democratic peace apply in the cyber sphere? Geiger (2021) conducted a quantitative analysis finding preliminary support of both the democratic and capitalist peace in cyberspace. Using cyberattack data from several sources, Geiger found that democratic dyads and capitalist dyads indeed appear to be less likely to engage in cyber conflict with one another, albeit acknowledging that that only having access to publicly known cyberattacks is a major limiting factor in the study.

This paper will extend the concept of the democratic peace to cyberattack attribution to assess how frequently democratic targets publicly point blame on other democracies for cyberattacks. The intent of this study of regime type impact on cyberattack attribution is not necessarily to prove a single cause of the democratic peace, but to explore to what extent and in what manner this pattern may extend the sphere of cyber conflict and attribution. It may be that when it is known that an actor from a democracy cyberattacks another democracy, the government of the targeted country withholds public attribution because it may be perceived as a public aggression. In this case, a government may handle retaliatory measures privately if it is unpopular to blame other democracies, if democratic institutions better facilitate private response, or if it reduces economic disruption.[1] This logic leads to the first empirical prediction:

H1: Democratic governments will be less likely to attribute perpetrators when a cyberattack originates from a democratic state.

Domestic Press Freedom as a Correlate of Public Attribution

Countries with high degrees of press freedom may be more inclined than those with fewer freedoms to publicly attribute cyberattacks because their governments are

[1] Note that popular existing models for the democratic peace, such as audience costs and bargaining, are difficult to apply to cyberattack attribution because they often rely on the considerations of the initiating state. This study instead primarily explores the considerations of the target state after an attack has already been initiated.

compelled into transparency. Egloff and Smeets (2023) note that “the secrecy of one’s own victim status will often be honored by security companies, but not by the media,” and that media entities narrow a government’s choices about when and how to make public attributions. The less confident a government is in its ability to control the spread of information about an attack, they argue, the more proactive governments will be about public attribution.

In the non-cyber realm, Lindstedt and Naurin (2010) similarly argue an association between press freedom and government operational transparency, finding a strong relationship between the two in political systems where leaders are held accountable through free elections. In a country with higher degrees of press freedom, a need to reveal information about an attack before non-government individuals and organizations shape the narrative through free means of communication may exist to maintain the government’s appearance of competence (Libicki 2009; Egloff and Smeets 2023). If a government is confident in its ability to prevent information and theories about an attack from spreading, it may refrain from making a public attribution to retain the benefits of non-attribution in public spaces. The logic above leads to the following empirical prediction:

H2: Governments of countries with higher degrees of press and expression freedom will be more likely to publicly attribute known cyberattacks than those with lower degrees of press and expression freedom.

EMPIRICAL METHODS

Data

Cyberattack data for this study originates from a 2023 dataset release from the European Repository of Cyber Incidents. This database includes 1644 global cyber incidents between 2000 and April 2023. The included incidents involve a violation of the "CIA triad of information security" and have been publicly reported by the target, attacker, or other third party. The CIA triad of information security states that a secure system a) is confidential, allowing only authorized access and disclosure, b) has integrity, secure against improper modification or destruction of information, and c) is available in a timely manner to those authorized to access it. Therefore, cyber incidents in which data confidentiality, data integrity, or data availability are compromised are included in the data.

The included incidents involve a political dimension: they "a) have affected political or state actors/institutions, b) have been associated with state-actors as the actual 'masterminds' or exhibit a political motivation, or c) have been 'publicly politicized, regardless of the affected target'" (EuRepoC 2023). Additionally, the dataset includes known attacks on critical infrastructure sectors, even if they do not have a political dimension. In this dataset, critical infrastructure attacks include attacks on the sectors of energy, water, transportation, health, chemicals, telecommunications, food, finance, defense industry, space, wastewater management, critical manufacturing, and digital providers. This paper refers to these incidents as "cyber conflict" rather than "cyber warfare"; while many of the included incidents occurred congruently with conventional warfare, the threshold of warfare in cyber conflict is subjective.

The 2023 EuRepoC data is extracted from 220 international media sources, as well as government websites, IT reports, and social media websites. The data is gleaned and initially processed through a machine-learning model where researchers then manually code data points. As with any manual or machine learning data collection process, there is a risk that some cases of publicly known cyberattacks were not captured by this process, which is an acknowledged limitation of the data. This does not necessarily invalidate the data, though; we may find that cyberattack cases that were insignificant enough to not be written about in online sources were also relatively unnoticed by the public, and as this research attempts to study public perception of cyberattacks, the data is still adequate for use in studying the hypotheses.

EuRepoC provides a multitude of details about each attack, including targeted countries and suspected initiators if known; some attacks have multiple targets and initiators. The dataset additionally details the sector of each attack and provides instances of attribution by any actor. Some attacks have no attribution, some have an attribution made by one actor, and some attacks are attributed by multiple entities such as governments and private companies.

A clear limitation of this data is that cyber incidents not known to the public cannot be included. While this study would be more comprehensive if such cases could be included, the limited scope of this data can still be used to test the above hypotheses. Because this study in part explores the audiences and media of targeted states, cyber incidents that have not been discovered or have been kept completely out of the public eye are not as relevant as those that are publicly known; this study is primarily interested in cases where there was a publicly known cyberattack and how the targeted state chose to respond.

Dependent Variable and Model Selection

This research employs bivariate logistic regressions to assess the relationships between public cyberattack attribution and the predictor variables proposed in the hypotheses. The unit of analysis used in this study is incident-dyad for H1 and incident-country for H2. Some incidents target multiple countries and are therefore separated so that the variance of each targeted country can be assessed. For each unit, a code is added for whether the government of the targeted country made a public attribution in that scenario as captured in the dataset. If an attack was not publicly attributed by a government actor, that likely means that the targeted entity was unable to make an attribution or that the incident was privately attributed out of view of the public.

Independent Variables

Each incident is compared with several data points to test the hypotheses. For the study of regime type and conflict dyads, the Freedom House report on whether each country is an electoral democracy, coded as yes or no, is used for each year from 2000 to 2023. For measures of civil liberties and government attribution, instances of cyber incidents are tested against each target country's press freedom score from Reporters Without Borders and the Freedom of Expression rating from V-Dem for each attack year.

The index from Reporters Without Borders combines measures of support for media autonomy from state and political actors, levels of journalistic freedom, economic constraints on the media, social constraints on journalists, and the safety of journalists. The V-Dem rating of expression freedom measures the extent to which the government of a country respects press and media freedom and the freedom of ordinary people to discuss political matters publicly and privately. All of these measures capture factors that may contribute to the proliferation of information about cyber incidents and, therefore, may impact a government’s decision to publicly attribute an incident. In this model, these two measures are combined into a Press & Expression Freedom score to capture the details of both indexes. This variable ranges from 0-2, with 0 being the lowest level of freedom and 2 being the highest.

Control Variables

Control variables are included to account for confounding relationships. The first control is a measure of the intensity of each incident, as it is likely that governments will be more inclined to attribute attacks that are more serious, salient, or far-reaching (Rid and Buchanan, 2014). More severe attacks naturally attract more attention and cause more harm, creating pressure for the incident to be addressed. The intensity of each incident is calculated by EuRepoC (2023) as a multiplication of the incident’s type, degree of disruption, physical effects, and target importance.

Second, I control for the percentage of people in a country that use the internet as a proxy for the salience of computer technology to a country. Countries with greater access to and investment in digital technology may be more inclined and have a greater capacity to investigate and attribute cyberattacks than those with less. This measure may also capture the availability of computer technology specialists to a government, a likely predictor of attribution. I source data from the World Bank’s measure of the percentage of individuals using the internet per country per year.

The GDP per capita of each country during the year of the attack is included to account for variations in income as a proxy measure for investigative ability. Wealthier countries may have a greater capacity to fund cyberattack investigations, as investigations require extra personnel, equipment, and training. GDP data is primarily sourced from The

World Bank and is supplemented with data from the International Monetary Fund in cases of missingness.

Models testing Hypothesis 1 control for several measures of cooperative relationships between dyads, as it may be that allied dyads are less likely to publicly attribute incidents between one another. Data is sourced from the Formal Alliances dataset from Correlates of War. The included variables list a) whether each dyad has engaged in an agreement of non-aggression, B) whether each dyad has agreed to remain neutral in case of a conflict involving the other, and C) whether each dyad has engaged in a defense pact in which they pledge to defend one another in case of military conflict. These variables will demonstrate whether relationships found in the analyses are due to regime type or simply due to existing alliances. Tables 1 and 2 provide descriptive statistics for the variables used in both models.

Table 1:
Variable Descriptive Statistics – Press Freedom Models

Statistic	Mean	SD	Min	Max	Median
Government Attribution	0.43	0.49	0	1	0
Target GDP per capita, USD	27523	22672	125	116787	29675
Weighted Cyber Intensity	2.575	1.12	0	10	3
Freedom of Press and Expression Index	1.28	0.49	0.06	1.99	1.34
Percent of Targeted Country Population Using Internet	87.48	15.05	0.1	120.7	93.4
Sample Size = 3847					

Table 2:
Variable Descriptive Statistics – Regime Dyad Models, Democratic Targets

Statistic	Mean	SD	Min	Max	Median
Government Attribution	0.21	0.41	0	1	0
Target GDP per capita, USD	38410	22324	223	116787	29675
Weighted Cyber Intensity	2.19	1.19	0	6	2
Initiator Regime Type	0.1	0.3	0	1	0
Percent of Targeted Country Population Using Internet	87.71	10.3	41.2	108.1	93.4
Non-Aggression Agreement	0.04	0.21	0	1	0
Neutrality Agreement	0.02	0.14	0	1	0
Defense Agreement	0.03	0.16	0	1	0
Sample Size = 876					

Unquantifiable variations among countries and regions may influence statistical results and are addressed with region fixed effects, an aid in accounting for a variety of important domestic and regional contexts. Additionally, year fixed effects are added to reduce the impact of other latent variables that vary year by year.

EMPIRICAL MODEL

Regime Type Dyads

An analysis of cyberattack data against dyad regime types reveals several patterns of interest. The number of cyber conflict dyads between democracies includes 86 incidents originating from democratic countries that reached democratic targets. Of these attacks, 39 are suspected to be sponsored directly by governments, 5 supported but not created by governments, and 45 by non-state actors. Of these incidents, seemingly only 5 state-sponsored incidents were publicly attributed by the targeted country’s government. This is in contrast to incidents targeting democracies initiated by actors in non-democracies in which there were hundreds of known cases, and a much higher proportion were attributed by the receiver government. Dyad frequencies are displayed in Figure 1.

Figure 1:
Frequencies of Known Initiator Regime Type and Initiator State Affiliation

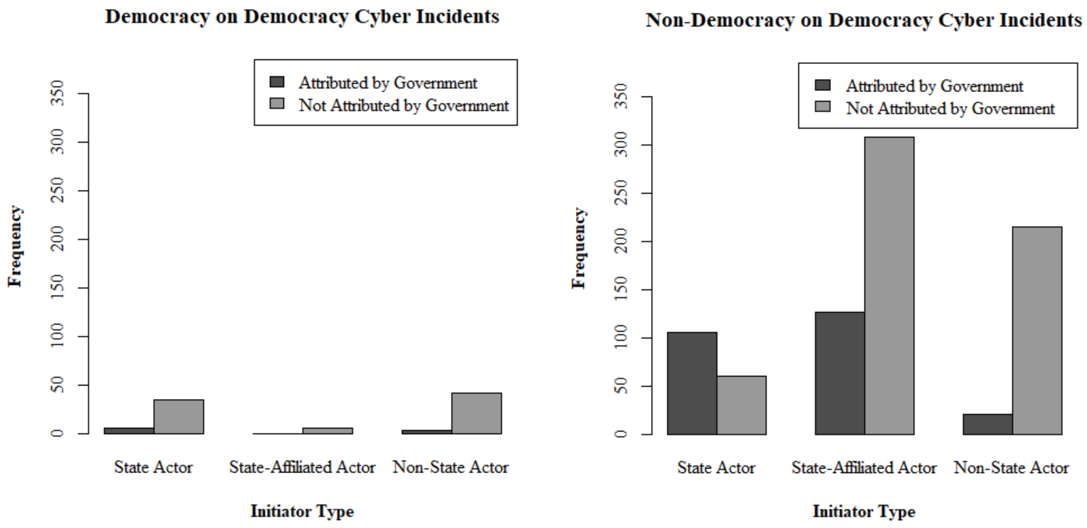


Table 3 summarizes the outputs of a logistic regression comparing log odds of attribution to initiator regime types among targeted democracies. In the Initiator Regime Type variable, 0 represents non-democracies and 1 represents democracies. Note that these models only include incidents where the country or countries of the suspected initiators have been attributed by some actor, including third parties. Cases where the country of the initiating actor is unknown to the public are not included.

Table 3:
Change in Log Odds of Public Attribution Among Democratic Targets, State and State-Affiliated Initiators

Model	(1)	(2)	(3)
Initiator Regime Type	-1.410*** (0.446)	-2.455*** (0.630)	-2.391*** (0.678)
Weighted Cyberattack Intensity		0.518*** (0.093)	0.512*** (0.093)
Percent of Targeted Country with Internet Access		0.013*** (0.016)	0.005 (0.016)
Target GDP per Capita, in thousands USD		0.01 (0.01)	0.01 (0.01)
Neutrality Agreement			2.334* (1.237)
Defense Agreement			-0.336 (0.955)
Non-Aggression Agreement			-1.445 (1.175)
N	613	613	613
AIC	840	726	726

**p<0.1; **p<0.05; ***p<0.01*
Models 2 and 3 include fixed effects for target country region and incident resolution year

This model reveals a difference in treatment among initiator regime types depending on the state affiliation of the initiating actor. Democracies appear significantly more likely to publicly attribute attacks suspected to have originated in non-democracies than those originating from democracies when the initiator has state ties. If public cyberattack attribution may be seen as an escalation of conflict, then this model is consistent with democratic peace theory.

The lack of public cases of democracy-on-democracy incidents may lend validity to democratic peace theory in the initiation of cyber conflict. Democracies rarely engage in cyber conflict with one another in the public eye. All cases of state-sponsored incidents in democratic dyads are cases of espionage, with two also involving data misuse by the initiator. Espionage is typically considered a less-severe form of attack than those involving data destruction, denial, or manipulation. Some literature attempts to place secret or covert actions between democracies in the context of the democratic peace; it may be that acts of espionage or other covert actions are an attempt to address conflicts without the cost of further escalation (Russet 1994). The lack of public attribution of these incidents further supports the theory that cyber operations, especially espionage, are a method of addressing conflict that is intended to occur privately.

Table 4 summarizes the output of a regression comparing of incidents on non-state actors targeting democracies based on the regime type of the initiator's home country. This model does not provide evidence of a difference in attribution based on the regime type of the initiator home country when the initiator is not affiliated with a state. This difference in the treatment of state and non-state actors is theoretically important: cyber conflict literature frequently notes the difficulty of distinguishing state and non-state actors. If this regression accurately represents the behavior of attributing actors, however, the similar reaction to all non-state actors regardless of the regime type of their home country provides evidence of a perception of separation of citizens and their governments when engaging in cyber conflict.

The same statistical analysis on cyber incidents targeting non-democracies also did not provide evidence ($p < 0.05$) of differences in attribution depending on the initiator regime type for both state and non-state actors (see appendix tables 8 and 9), further suggesting that this difference is exclusive to democracies targeted by non-democracies.

Table 4
Change in Log Odds of Public Attribution Among Democratic Targets, Non-State Affiliated Initiators

Model	(1)	(2)	(3)
Initiator Home Country Regime Type	-0.0718 (0.759)	-1.199 (1.027)	-1.621 (1.142)
Weighted Cyberattack Intensity		0.479* (0.252)	0.524** (0.264)
Percent of Targeted Country with Internet Access		0.049* (0.047)	0.059 (0.060)
Target GDP per Capita, in thousands USD		0.01 (0.02)	0.01 (0.02)
Neutrality Agreement			19.941 (2332)
Defense Agreement			3.786** (1.712)
Non-Aggression Agreement			-18.909 (2332)
N	263	263	263
AIC	161	154	154

**p<0.1; **p<0.05; ***p<0.01*
Models 2 and 3 include fixed effects for target country region and incident resolution year

Press Freedom Among Targeted States

Figure 2 displays the distribution of press & expression freedom scores among countries that experienced at least one cyberattack as listed in EuRepoC’s 2023 dataset. While the distribution has a somewhat leftward skew, it is not excessive. Democracies have mostly higher scores and non-democracies mostly lower scores, indicating that there is likely an association between regime type and odds of attribution; press freedom is the proposed causal mechanism of the hypothesis, however.

Figure 2*:*
Frequency of Press & Expression Freedom Scores Among Targeted States

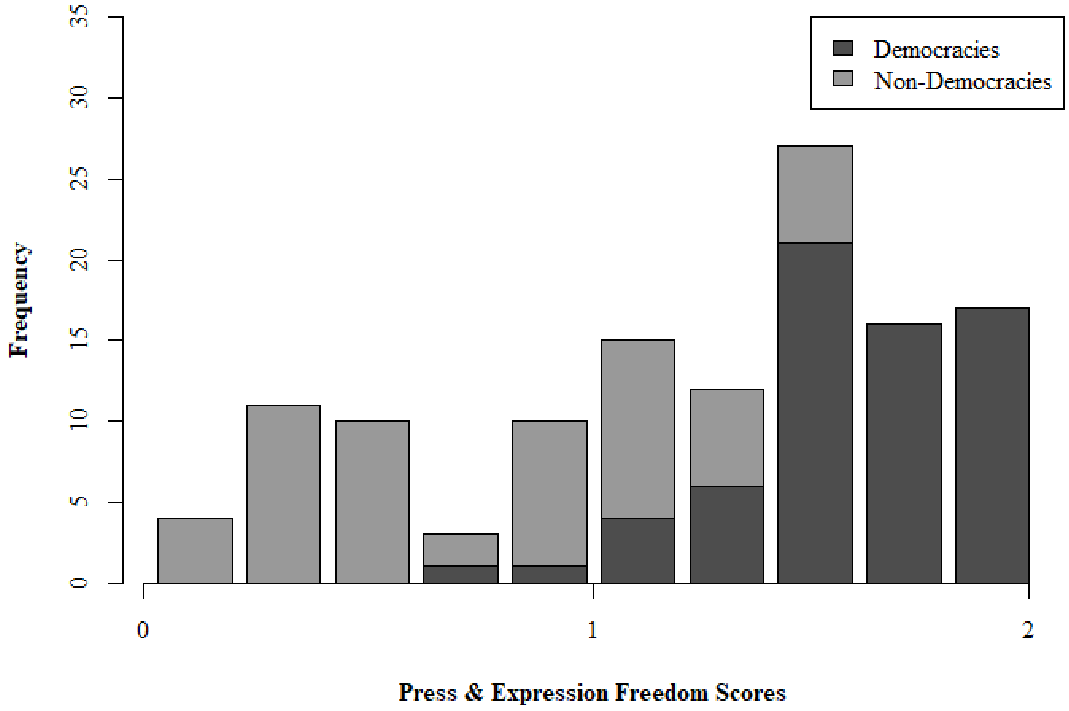


Table 5 summarizes the output of a logistic regression comparing log odds of public attribution to the press & expression freedom index score for each targeted country in the year of the incident. There were 3847 observations of targeted countries included in each regression. All models display a statistically significant positive association between index scores and odds of attribution ($p < 0.01$). There are also, as expected, positive associations between the control variables and odds of attribution.

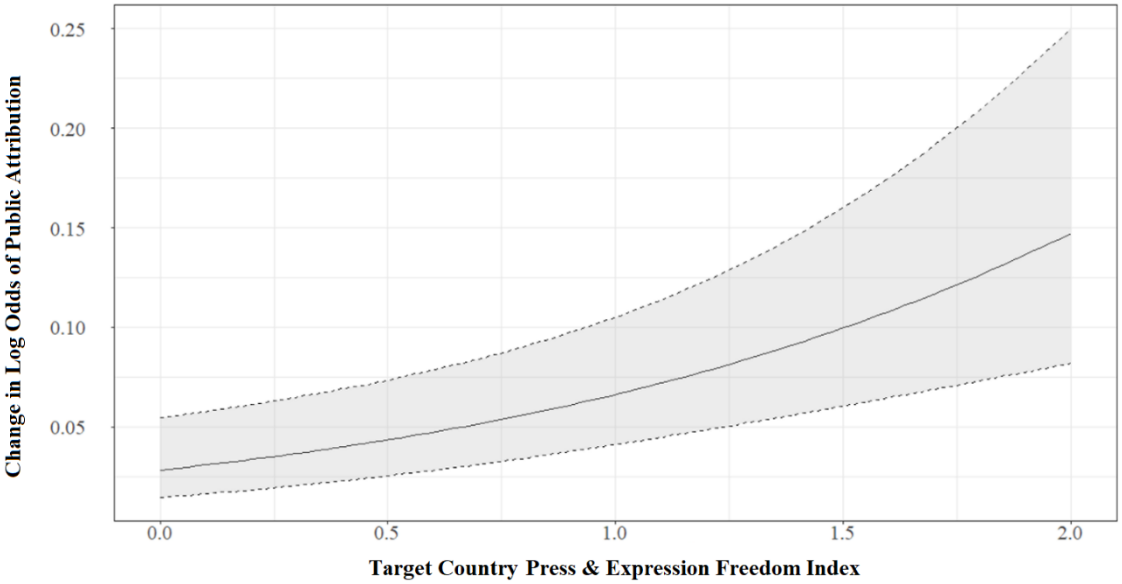
Table 5:
Domestic Press Freedom and Log Odds of Public Attribution

Model	(1)	(2)	(3)
Freedom of Expression And Press Index, Targeted Country	1.068*** (0.120)	1.189*** (0.142)	0.890*** (0.226)
Weighted Cyberattack Intensity		0.505*** (0.041)	0.673*** (0.053)
Percent of Targeted Country with Internet Access		0.054*** (0.007)	0.039*** (0.008)
GDP per Capita, in thousands USD			0.002 (0.004)
N			3847
AIC	5714	4797	2511

**p<0.1; **p<0.05; ***p<0.01*
Model 3 includes fixed effects for target country region and incident resolution year

Figure 3 displays the predicted probabilities of attribution in log odds depending on the domestic press freedom of the targeted country. These predicted probabilities use the same control variables as Model 3 of Table 5, including the attack intensity, percent of targeted country with internet access, and GDP per capita. The log odds of attribution at a minimum press and expression freedom score of 0 are 0.027, while the log odds of attribution at a maximum press and expression freedom score of 2 are 0.211. There is therefore a 0.184 log odd difference between odds of public attribution among the most and least free states.

Figure 3:
Press & Expression Freedom and Cyberattack Attribution Log Odds



While there are other factors associated with these cases that may have impacted each country's odds of attribution, this model provides preliminary evidence that the risk of incident information spreading freely through the media motivates public attribution for government actors. Conversely, governments that can confidently prevent the spread of incident information may prefer to retain the benefits of refraining from public attribution. If a government is not compelled into attribution transparency by a free press, it may prevent the exposure of vulnerabilities and avoid pressure to retaliate against its strategic interests.

CASE STUDIES

High-profile cases of cyberattacks illustrate the behavior and decision-making process of state actors following cyber incidents. Instances of cyberattacks on the healthcare systems of Singapore and South Korea, as well as a case of espionage on South Korean officials, demonstrate decision making parallel to the above empirical findings. While these case studies involve contexts that cannot be quantified nor fully explained in this study, they demonstrate attribution patterns important to the understanding of cyber conflict.

Table 6:
Case Study Comparisons

Target Country	**Singapore**	**South Korea**	**South Korea**
Target Type	Healthcare	Healthcare	Government Communication
Press Freedom	Lower	Higher	Higher
Dyad	Non-Democracy on Non-Democracy	Non-Democracy on Democracy	Democracy on Democracy
Public Attribution by Government Actors?	No	Yes	No
Justification	Preservation of national security		Concerns that the incident was fabricated

Low Press Freedom: Singaporean Health Services Breach

Singapore’s most severe cyberattack in national history was that on Singaporean medical network SingHealth. Between May and July of 2018, hackers breached over 1.5 million health records in the network. Singapore’s Ministry of Health reported that names, addresses, races, and dates of births of patients were leaked, although the provision of health services was uninterrupted (Tham 2018). The tools used in the attack were specially tailored to breach the anti-malware software and security tools of SingHealth with the intent of disclosing patient information (CNA 2018).

Following the attack, Singaporean officials publicly stated that the attack was perpetrated by an advanced persistent threat (APT) group. They said that it was likely backed by a nation-state and was highly sophisticated. In a series of statements, Minister for Communications and Information S Iswaran deliberately did not state who investigators believed to be the actor or host of the APT (Kim 2018). He explained that “for national security reasons we will not be making any specific public attribution” (CNA 2018). He also warned Singapore’s parliament against assigning blame for the attack: “I would urge members to refrain from going down the path of allocating blame at this point,” as “some aspects of the inquiry have security implications, the [Committee of Inquiry] will decide which part of its hearings can be held in public” (Osman 2018).

Singhealth’s data breach and subsequent non-attribution can be analyzed through the pattern of attribution and press freedom found in the quantitative analysis. Singapore is rated low in measures of press freedom afforded by government, and because of that state officials may be more confident that the decision to avoid public attribution will achieve the benefits of non-attribution. Singapore has the authority to take legal action against journalists if their reporting threatens national security or if reporting is involved in "serious incidents." Part of Singapore's posited justification for the suppression of free press is the preservation of state security (Freedom House 2022; Singapore Status Online 2024). Since most of Singapore's news media is state-affiliated or under strong state regulation, there was essentially no speculation of the initiating country in prominent Singaporean-owned news media.

This case is congruent with the risk-benefit analysis that states may engage in when deciding whether to publicly attribute an attack. By avoiding public attribution, Singapore may have prevented the exposure of vulnerabilites (especially in the sensitive healthcare sector), protected information sensitive to the investigation, and protected themselves from being pressured into a retaliation that would be against their strategic interest, while being reasonably confident that unfounded narratives would not spread.

The remainder of Singapore's response to this incident was kept private. No public attribution of the perpetrators of the attack was ever made by government officials, although several foreign cybersecurity companies attributed the attack to Chinese actors (Symantec 2019). If the attack indeed originated from China, there were clearly other historical and political contexts that contributed to this response, but press freedom may have in part contributed to the government's confidence in the decision to avoid public attribution.

High Press Freedom: South Korean Health Services Breach

A strikingly similar attack on health services in South Korea demonstrates a different set of circumstances that may have contributed to the decision of public attribution by state officials. In March of 2023, a cyberattack breached the medical data of over 1 million patients at the Seoul National University Hospital. The breach similarly revealed patient health information but did not interrupt the provision of healthcare at the hospital (Paganini 2023).

Following the attack, the Korean National Police Agency made public statements attributing the attack to a nation-state actor. They specifically attributed the incident to North Korean hackers, describing the tactics, techniques, and procedures of the incident. They described the IP addresses and language markers that distinguished North Korean hackers from those of other threat actors and facilitated the forensic process (Marshal 2023; Korean National Police 2023).

The level of detail provided is notable because the Korean National Police Agency revealed information that could expose the health agency or other entities to more cyber risks as it revealed vulnerabilities in systems and cybersecurity approaches (Paganini 2023). Government leaders may have decided, however, that the benefits of publicly attributing the attack were greater than the potential risks.

The decision to make a public attribution may have in part been due to a confidence that speculation on the incident would have spread regardless of the government's attribution decision—South Korea scores higher than most countries in measures of press and expression freedom (Freedom House 2024). Due to the sensitive nature of the data leaked, South Korea's government may have paid a higher cost by not making an attribution than by making an attribution, particularly given national perceptions of North Korea and their contentious conflict history.

Democratic Dyad: US Espionage on South Korea

As shown in the quantitative analysis, there are few publicly known cases of democracy-on-democracy cyber incidents. This may be due to a real lack of attacks between democratic dyads or due to a propensity of targeted democracies to keep such incidents private. One publicly known cyber incident, however, targeted South Korea in 2023 and was suspected to have been initiated by the United States. A series of leaked documents, which were exposed by an anonymous actor with access to sensitive intelligence information, demonstrated that the US may have engaged in clandestine espionage on South Korean executive leaders by intercepting sensitive communication data. The leaked documents detailed the opinions and considerations of South Korean officials on aid to Ukraine during the Russo-Ukrainian war, which could have been acquired only through the illicit interception of data. This case was made known to the public through leaked documents spread on 4chan, Discord, and to the New York Times (Guyer 2023; Sang-Hun 2023).

In a press statement, South Korean president Yoon Suk Yeol denied that the leaked documents were accurate and denied that the US engaged in cyber espionage on South Korea. Yoon assured the public that his administration has strong safeguards against foreign espionage and posited that the leaked documents were fabricated by the American party that leaked them. Officials refused to discuss which parts of the leaked documents they suspected to be fabricated, however (Gallo and Juhyun 2023; Sang-Hun 2023).

Yoon's political opponents argued that Yoon's administration should take stronger retaliatory measures against the US for the intrusion (Kim 2023). Yoon argued in response that such opponents were attempting only to undermine South Korea's relationship with the US and make his administration look incompetent, accusing them of "spreading 'fake, negative suspicions' in order to gin up votes" (Sang-Hun 2023).

Despite South Korea's denial of the validity of the documents and reassurance that the US has not engaged in cyber incidents against South Korea, there is a high likelihood that the reports of espionage are accurate, especially as US FBI officials confirmed that the leaked documents seemed to be legitimate Pentagon intelligence documents, even if some were altered (Sang-Hun 2023; McCurry et al. 2023). Why, then, was there such vehement denial of the incident by South Korean officials?

This case may be an instance of an extension of the democratic peace into the realm of cyberattack attribution in that both parties were democracies and no public attribution was made. While this study does not suggest a single cause of the democratic peace in the context of cyberattack attribution, Yoon appeared concerned that South Korea being framed as a target by politically similar countries would make the administration look incompetent. He explicitly stated that the ordeal was an attempt to cause his administration to lose votes in the next election. If normative or structural explanations for the democratic peace are accurate, it may be that attributing the US as a perpetrator in this attack would be perceived poorly due to the shared political norms or political structures between South Korea and the US. While attacks from countries like North Korea are expected and promptly responded to, publicizing attacks from the US may be unexpected or unpopular.

Case Study Discussion

Cyberattacks targeting Singapore and South Korea provide insight into the contexts of public cyberattack attribution. These cases are not precisely parallel; each involves complicated relationships between the perpetrator and target and different public perceptions. Existing alliances, the identity of cyberattack initiators, adversarial relationships, and geography contribute to cyber conflict perceptions. In the cases targeting South Korea, for example, North Korea is an existing threat to nationhood while the US is closer politically with a converse power dynamic. Rather than proposing a simple cause of public attribution or non-attribution, these cases demonstrate the complexity of the attribution process, which appears to in part be a result of domestic opinion and norms. Future case studies will provide additional considerations in the attribution process.

CONCLUSION

The relationships found in these models and cases present novel findings in cyberattack attribution research. While it is known that forensic capability and conflict strategy contribute to a government's decision to publicly attribute cyberattacks, domestic political contexts likely also contribute to this decision.

Not only do publicly known cyberattacks between those in democracies appear far less frequently than those originating from non-democracies, but the data suggest that they are publicly attributed by democratic governments less frequently. This finding is consistent with some explanations for the democratic peace. If cyberattack attribution is to be viewed as a step of conflict, perhaps democratic leaders avoid attribution as they worry how their constituents will view the publicization or escalation of conflict with other democracies. Alternatively, it may cause economic uncertainty or disruption, or structural factors associated with democracy may favor private resolution with one another over public resolution (Tomz and Weeks 2013; Gartzke 2007). Further research would be necessary to understand receiver-side explanations for the avoidance of public attribution when democracies target other democracies.

Additionally, the data is consistent with the hypothesis that greater degrees of press freedom are associated with an increased odds of cyberattack attribution. This association holds even controlling GDP, internet access within the targeted country, and incident severity. This relationship suggests that governments may feel compelled to discuss the details of cyber incidents publicly when they know that news and media sources will report on the incident whether or not the government makes a public attribution (Egloff and Smeets 2023).

Case studies of cyberattacks on Singapore’s health system, South Korea’s health system, and South Korea’s leadership demonstrate some of these patterns. Singaporean officials were deliberately silent about the perpetrators of a large cyberattack on their health system, warning that public attribution by the government or third parties would be a national security risk, while a similar attack on freer South Korea’s health system resulted in prompt public attribution by government officials. In a case of suspected American espionage on South Korean officials, however, governments actors denied that there was an incident and denied that the US breached any systems, blaming those perpetuating the idea for trying to undermine the administration’s credibility and diplomatic ties.

From these findings, we may deduce that greater incentives for public cyberattack attribution among state actors exist when the targeted state has high degrees of press freedom and when they are a democracy targeted by a non-democracy. While many factors influence the decision to make public attributions, domestic political circumstances appear to contribute in part to this choice. These findings create an opportunity for further study on the domestic political circumstances that affect the decisions of state actors to publicly attribute the perpetrators of cyberattacks.

As these cases are observational and may be impacted by other confounding variables, additional cases studies and other qualitative research would be an appropriate supplement to assess the internal validity of these findings, especially as individual cyber incidents involve unique nuances and contexts that are difficult to quantify. It will also be appropriate to compare these findings across cyber incident data as more is made available, particularly if data about attribution decision making is eventually declassified by governments. Continuing research in the domain of cyber conflict will aid in building an understanding of the perceptions and risks surrounding cyber conflict in the digital age, whether cyberattacks remain a tool of conflict or become a primary method of fighting conflict.

BIBLIOGRAPHY

Acton, James M. “Cyber Warfare & Inadvertent Escalation.” *Daedalus* 149, no. 2 (2020): 133–49. https://doi.org/10.1162/daed_a_01794.

Adiputera, Yunizar. “Evaluating the Normative and Structural Explanations of Democratic Peace Theory.” *Global South Review* 1, no. 1 (October 9, 2017): 21. https://doi.org/10.22146/globalsouth.28817.

Baram, Gil, and Udi Sommer. “Covert or Not Covert: National Strategies During Cyber Conflict.” In *2019 11th International Conference on Cyber Conflict (CyCon)*, 1–16. Tallinn, Estonia: IEEE, 2019. https://doi.org/10.23919/CYCON.2019.8756682.

Boerbert, W. Earl. “A Survey of Challenges in Attribution.” In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy*. Washington, D.C.: National Academies Press, 2010. https://doi.org/10.17226/12997.

Canfil, Justin Key. “The Illogic of Plausible Deniability: Why Proxy Conflict in Cyberspace May No Longer Pay.” *Journal of Cybersecurity* 8, no. 1 (January 28, 2022). https://doi.org/10.1093/cybsec/tyac007.

Clement, Guitton. “Criminals and Cyber Attacks: The Missing Link between Attribution and Deterrence.” *International Journal of Cyber Criminology* 6 (2012). https://www.academia.edu/download/30971316/guiton2012julyijcc.pdf.

Czosseck. “State Actors and Their Proxies in Cyberspace.” In *Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy*, edited by Katharina Ziolkowski. Tallinn, Estonia: NATO CCD COE Publ, 2013.

Demchak, Chris. “Cybered Conflict vs. Cyber War.” *Atlantic Council* (blog), October 20, 2010. https://www.atlanticcouncil.org/blogs/new-atlanticist/cybered-conflict-vs-cyber-war/.

De Mesquita, Bruce Bueno, James D. Morrow, Randolph M. Siverson, and Alastair Smith. “An Institutional Explanation of the Democratic Peace.” *American Political Science Review* 93, no. 4 (1999): 791–807. https://doi.org/10.2307/2586113.

Deeks, Ashley. “The Geography of Cyber Conflict: Through a Glass Darkly.” SSRN Scholarly Paper. Rochester, NY, March 14, 2013. https://papers.ssrn.com/abstract=2233560.

Dipoppa, Gemma, and Guy Grossman. “The Effect of Election Proximity on Government Responsiveness and Citizens’ Participation: Evidence From English Local Elections.” *Comparative Political Studies* 53, no. 14 (2020): 2183–2212. https://doi.org/10.1177/0010414020912290.

Dunn Cavelty, Myriam, and Andreas Wenger. “Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science.” *Contemporary Security Policy* 41, no. 1 (January 2, 2020): 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Edwards, Benjamin, Alexander Furnas, Stephanie Forrest, and Robert Axelrod. “Strategic Aspects of Cyberattack, Attribution, and Blame.” *Proceedings of the National Academy of Sciences* 114, no. 11 (March 14, 2017): 2825–30. https://doi.org/10.1073/pnas.1700442114.

Egloff, Florian J. “Public Attribution of Cyber Intrusions.” *Journal of Cybersecurity* 6, no. 1 (January 1, 2020): tyaa012. https://doi.org/10.1093/cybsec/tyaa012.

Egloff, Florian J, and Myriam Dunn Cavelty. “Attribution and Knowledge Creation Assemblages in Cybersecurity Politics.” *Journal of Cybersecurity* 7, no. 1 (February 16, 2021): tyab002. https://doi.org/10.1093/cybsec/tyab002.

Egloff, Florian J., and Max Smeets. “Publicly Attributing Cyber Attacks: A Framework.” *Journal of Strategic Studies* 46, no. 3 (April 16, 2023): 502–33. https://doi.org/10.1080/01402390.2021.1895117.

Eichensehr, Kristen E. “The Law and Politics of Cyberattack Attribution.” UCLA Law Review, 2020.

EuRepoC: European Repository of Cyber Incidents. “EuRepoC Database.” Accessed November 13, 2023. https://eurepoc.eu/database/.

Farwell, James P., and Rafal Rohozinski. “Stuxnet and the Future of Cyber War.” *Survival* 53, no. 1 (2011): 23–40. https://doi.org/10.1080/00396338.2011.555586.

Fearon, James D. “Domestic Political Audiences and the Escalation of International Disputes.” *American Political Science Review* 88, no. 3 (1994): 577–92. https://doi.org/10.2307/2944796.

Freedom House. “Freedom on the Net.” Accessed November 13, 2023. https://freedomhouse.org/report/freedom-net.

Freedom House. “Singapore: Freedom on the Net 2022 Country Report.” Accessed March 31, 2024. https://freedomhouse.org/country/singapore/freedom-net/2022.

Freedom House. “South Korea: Freedom in the World 2024 Country Report.” Accessed April 1, 2024. https://freedomhouse.org/country/south-korea/freedom-world/2024.

Full Ministerial Statement on SingHealth Cyberattack by S Iswaran. CNA, 2019. https://www.youtube.com/watch?v=VPnZk9Ckjw4.

Gallo, William, and Lee Juhyun. "Ahead of Biden-Yoon Meeting, US Accused of Spying on South Korea." Voice of America, April 10, 2023. https://www.voanews.com/a/ahead-of-biden-yoon-meeting-us-accused-of-spying-on-south-korea/7043685.html.

Gandhi, Robin, Anup Sharma, William Mahoney, William Sousan, Qiuming Zhu, and Phillip Laplante. "Dimensions of Cyber-Attacks: Cultural, Social, Economic, and Political." *IEEE Technology and Society Magazine* 30, no. 1 (2011): 28–38. https://doi.org/10.1109/MTS.2011.940293.

Gartzke, Erik. "The Capitalist Peace." *American Journal of Political Science* 51, no. 1 (2007): 166–91. https://www.jstor.org/stable/4122913.

Geers, Kenneth. "The Challenge of Cyber Attack Deterrence." *Computer Law & Security Review* 26, no. 3 (2010): 298–303. https://doi.org/10.1016/j.clsr.2010.03.003.

Geiger, Johannes. "The Democratic and Capitalist Peace in Cyberspace." *Pax et Bellum Journal*, no. 8th (2021). http://www.paxetbellum.org/wp-content/uploads/2021/06/Journal-with-cover.pdf.

Goel, Sanjay. "How Improved Attribution in Cyber Warfare Can Help De-Escalate Cyber Arms Race." *Connections* 19, no. 1 (2020): 87–95. https://www.jstor.org/stable/26934538.

Guyer, Jonathan. "The Ongoing Scandal over Leaked US Intel Documents, Explained." Vox, April 10, 2023. https://www.vox.com/world-politics/2023/4/10/23677820/leaked-intelligence-documents-ukraine-war-discord-4chan.

Healy, Jason. "Beyond Attribution: Seeking National Responsibility in Cyberspace." *Atlantic Council* (blog), February 22, 2012. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/.

Hinde, Stephen. "Cyber Wars and Other Threats." *Computers & Security* 17, no. 2 (1998): 115–18. https://doi.org/10.1016/S0167-4048(97)81979-7.

Kim, Jack. "Cyberattack on Singapore Health Database Steals Details of 1.5 Million, Including PM." *Reuters*, July 20, 2018, sec. Technology. https://www.reuters.com/article/idUSKBN1KA14B/.

Kim, Min Joo. "South Korea Says Leaked U.S. Documents Were 'Altered' and Are 'Untrue.'" *Washington Post*, April 11, 2023. https://www.washingtonpost.com/world/2023/04/11/south-korea-leaked-document-ukraine/.

Korean National Police. “Seoul National University Hospital Hacking and Personal Information Leakage Incident North Korea’s Fault,” May 11, 2023. https://www.police.go.kr/viewer/skin/doc.html?fn=d6c2795c-3930-44ab-970d-d2d7a14f9571.hwpx&rs=/viewer/202305.

LeVeck, Brad L., and Neil Narang. “The Democratic Peace and the Wisdom of Crowds.” *International Studies Quarterly* 61, no. 4 (2017): 867–80. https://www.jstor.org/stable/48539059.

Liang, Annabelle. “Singapore Says It Won’t Name Hackers Who Targeted PM.” AP News, January 15, 2019. https://apnews.com/general-news-bb334ef816a948e5aa6ddefae584e03e.

Libicki, Martin C. *Cyberdeterrence and Cyberwar*. Rand Corporation Monograph Series. Santa Monica, California: RAND Corporation, 2009.

Lindstedt, Catharina, and Daniel Naurin. “Transparency Is Not Enough: Making Transparency Effective in Reducing Corruption (La Transparence Ne Suffit Pas: Rendre La Transparence Efficace Dans La Lutte Contre La Corruption) (La Transparencia No Basta: Cómo Crear Una Transparencia Efectiva Para Reducir La Corrupción).” *International Political Science Review / Revue Internationale de Science Politique* 31, no. 3 (2010): 301–22. https://www.jstor.org/stable/25703868.

Maoz, Zeev, and Bruce Russett. “Normative and Structural Causes of Democratic Peace, 1946–1986.” *American Political Science Review* 87, no. 3 (1993): 624–38. https://doi.org/10.2307/2938740.

Marshal, William. “North Korean Hackers Breach Seoul National University Hospital.” *The Cybersecurity Times* (blog), May 11, 2023. https://www.thecybersecuritytimes.com/north-korean-hackers-breach-seoul-national-university-hospital/.

Maschmeyer, Lennart. “A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict.” *Journal of Strategic Studies* 46, no. 3 (April 16, 2023): 570–94. https://doi.org/10.1080/01402390.2022.2104253.

Maurer, Tim. *Cyber Mercenaries: The State, Hackers, and Power*. Cambridge New York, NY Port Melbourne New Delhi Singapore: Cambridge University Press, 2018.

McConnell, Mike. “Cyberwar Is the New Atomic Age.” *New Perspectives Quarterly* 26, no. 3 (2009): 72–77. https://doi.org/10.1111/j.1540-5842.2009.01103.x.

McCurry, Justin, Julian Borger, and Ben Doherty. “Pentagon Leaks: US Seeks to Mend Ties after Claims Washington Spied on Key Allies.” *The Guardian*, April 11, 2023, sec. US news. https://www.theguardian.com/us-news/2023/apr/11/pentagon-leaks-us-seeks-to-mend-ties-after-claims-washington-spied-on-key-allies.

Mousseau, Michael. “The Democratic Peace Unraveled: It’s the Economy ” *International Studies Quarterly* 57, no. 1 (2013): 186–97. https://doi.org/10.1111/isqu.12003.

Mueller, Milton, Karl Grindal, Brenden Kuerbis, and Farzaneh Badiei. “Cyber Attribution: Can a New Institution Achieve Transnational Credibility?” *The Cyber Defense Review* 4, no. 1 (2019): 107–22. https://www.jstor.org/stable/26623070.

Narang, Vipin, and Paul Staniland. “Democratic Accountability and Foreign Security Policy: Theory and Evidence from India.” *Security Studies* 27, no. 3 (July 3, 2018): 410–47. https://doi.org/10.1080/09636412.2017.1416818.

Nitzberg, S.D. “The Cyber Battlefield Is This the Setting for the Ultimate World War?” In *MILCOM 1999. IEEE Military Communications. Conference Proceedings (Cat. No.99CH36341)*, 1:707–13. Atlantic City, NJ, USA: IEEE, 1999. https://doi.org/10.1109/MILCOM.1999.822776.

Osman, Dhany. “SingHealth Cyberattack Fits Profile of ‘typically State-Linked’ Groups: Iswaran.” Yahoo News, August 6, 2018. https://sg.news.yahoo.com/singhealth-cyberattack-fits-profile-typically-state-linked-groups-iswaran-084512912.html.

Otto, Jacob, and William Spaniel. “Doubling Down: The Danger of Disclosing Secret Action.” *International Studies Quarterly* 65, no. 2 (June 8, 2021): 500–511. https://doi.org/10.1093/isq/sqaa081.

Owen, John M. “How Liberalism Produces Democratic Peace.” *International Security* 19, no. 2 (1994): 87. https://doi.org/10.2307/2539197.

Paganini, Pierluigi. “Non-State Actors in Cyberspace: An Attempt to a Taxonomic Classification, Role, Impact and Relations With a State’s Socio-Economic Structure.” Center for Cyber Security and International Relations Studies, June 2022.

———. “North Korean APT Breached Seoul National University Hospital.” Security Affairs, May 11, 2023. https://securityaffairs.com/146088/apt/seoul-national-university-hospital-hack.html.

Peterson, Andrea. “The Sony Pictures Hack, Explained.” *Washington Post*, December 18, 2014. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/.

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, D.C.: National Academies Press, 2010. https://doi.org/10.17226/12997.

Rathmell, Andrew. “Cyber-Terrorism: The Shape of Future Conflict?” *Journal of Financial Crime* 6, no. 3 (January 1, 1999): 277–83. https://doi.org/10.1108/eb025897.

Reich, Pauline C., Stuart Weinstein, Charles Wild, and Allan S. Cabanlong. "Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents – and the Dilemma of Anonymity." *European Journal of Law and Technology* 1, no. 2 (October 7, 2010). https://www.ejlt.org/index.php/ejlt/article/view/40.

Reiter, Dan. "Is Democracy a Cause of Peace?" In *Oxford Research Encyclopedia of Politics*, by Dan Reiter. Oxford University Press, 2017. https://doi.org/10.1093/acrefore/9780190228637.013.287.

Rid, Thomas. "Cyber War Will Not Take Place." *Journal of Strategic Studies* 35, no. 1 (2012): 5–32. https://doi.org/10.1080/01402390.2011.608939.

Rid, Thomas, and Ben Buchanan. "Attributing Cyber Attacks." *Journal of Strategic Studies* 38, no. 1–2 (January 2, 2015): 4–37. https://doi.org/10.1080/01402390.2014.977382.

Rosato, Sebastian. "The Flawed Logic of Democratic Peace Theory." *The American Political Science Review* 97, no. 4 (2003): 585–602. https://www.jstor.org/stable/3593025.

"RSF Index." Accessed November 13, 2023. https://rsf.org/en/index.

Russett, Bruce. *Grasping the Democratic Peace: Principles for a Post-Cold War World*. Princeton University Press, 1994. https://doi.org/10.2307/j.ctt7rqf6.

Sampanis, Spyridon, Melina-Eleftheria Spiliopoulou, Ioanna Kantzavelou, and Leandros Maglaras. "Cyberwarfare in the Modern World." In *Hybrid Threats, Cyberterrorism and Cyberwarfare*, by Mohamed Amine Ferrag, Ioanna Kantzavelou, Leandros Maglaras, and Helge Janicke, 1–21, 1st ed. Boca Raton: CRC Press, 2023. https://doi.org/10.1201/9781003314721-1.

Sanger, David E., and Nicole Perlroth. "U.S. Said to Find North Korea Ordered Cyberattack on Sony." *The New York Times*, December 17, 2014, sec. World. https://www.nytimes.com/2014/12/18/world/asia/us-links-north-korea-to-sony-hacking.html.

Sang-Hun, Choe. "Leaked Documents and Accusations of U.S. Spying Spark Outrage in Seoul." *The New York Times*, April 11, 2023, sec. World. https://www.nytimes.com/2023/04/11/world/asia/south-korea-leaked-pentagon-documents.html.

Sang-Hun, Choe. "Leaked Documents Show Seoul Torn Between U.S. Demands and Its Own Policy." *The New York Times*, April 9, 2023, sec. World. https://www.nytimes.com/2023/04/09/world/asia/leak-pentagon-south-korea-ukraine.html.

Schneider, Jacquelyn, Benjamin Schechter, and Rachael Shaffer. “A Lot of Cyber Fizzle But Not A Lot of Bang: Evidence about the Use of Cyber Operations from Wargames.” *Journal of Global Security Studies* 7, no. 2 (April 25, 2022): ogac005. https://doi.org/10.1093/jogss/ogac005.

Schulzke, Marcus. “The Politics of Attributing Blame for Cyberattacks and the Costs of Uncertainty.” *Perspectives on Politics* 16, no. 4 (2018): 954–68. https://doi.org/10.1017/S153759271800110X.

Singapore Statuses Online. “Telecommunications Act 1999,” 2024. https://sso.agc.gov.sg:5443/Act/TA1999.

Smith, Alastair. “Diversionary Foreign Policy in Democratic Systems.” *International Studies Quarterly* 40, no. 1 (1996): 133. https://doi.org/10.2307/2600934.

Stanton, Rich. “Self-Described Gay Furry Hackers Breach One of the Biggest Nuclear Labs in the US, and Demand It Begin Researching ‘IRL Catgirls.’” Yahoo Finance, November 23, 2023. https://finance.yahoo.com/news/self-described-gay-furry-hackers-175013075.html.

Symantec. “Whitefly: Espionage Group Has Singapore in Its Sights,” March 6, 2019. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/whitefly-espionage-singapore.

Thackray, Helen. “Hackers Gonna Hack: Investigating the Effect of Group Processes and Social Identities within Online Hacking Communities.” Bournemouth University, 2018. https://eprints.bournemouth.ac.uk/32219/1/THACKRAY%2C%20Helen_Ph.D._2018.pdf .

Tham, Irene. “Personal Info of 1.5m SingHealth Patients, Including PM Lee, Stolen in Singapore’s Worst Cyber Attack.” *The Straits Times*, July 20, 2018. https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most.

“The V-Dem Dataset.” Accessed November 13, 2023. https://v-dem.net/data/the-v-dem-dataset/.

Tomz, Michael R., and Jessica L. P. Weeks. “Public Opinion and the Democratic Peace.” *American Political Science Review* 107, no. 4 (2013): 849–65. https://doi.org/10.1017/S0003055413000488.

Tran, Delbert. “The Law of Attribution: Rules for Attributing the Source of a Cyber-Attack,” 20 Yale JL & Tech 376, 2018.

APPENDIX

Table 7:
Variable Descriptive Statistics – Regime Dyad Models, Non-Democratic Targets

Statistic	Mean	SD	Min	Max	Median
Government Attribution	0.013	0.11	0	1	0
Target GDP per capita, USD	9821	13823	125	98041	5607
Weighted Cyber Intensity	1.85	1.03	0	9	1
Initiator Regime Type	0.42	0.49	0	1	0
Percent of Targeted Country Population Using Internet	73.8	22.6	0.1	120.7	84.5
Non-Aggression Agreement	0.05	0.21	0	1	0
Neutrality Agreement	0.01	0.08	0	1	0
Defense Agreement	0.08	0.27	0	1	0
Sample Size = 408					

Table 8:

Change in Log Odds of Public Attribution Among Non-Democratic Targets, State and State-Affiliated Initiators

Model	(1)	(2)	(3)
Initiator Regime Type	-0.054 (0.428)	-1.746* (1.015)	-1.326 (1.061)
Weighted Cyberattack Intensity		0.318 (0.197)	0.353* (0.093)
Percent of Targeted Country with Internet Access		0.063** (0.028)	0.052* (0.028)
Target GDP per Capita, in thousands USD		0.01 (0.02)	0.01 (0.02)
Neutrality Agreement			-17.192 (17730)
Defense Agreement			1.032 (0.777)
Non-Aggression Agreement			-0.748 (1.346)
N	249	249	249
AIC	218	159	163

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

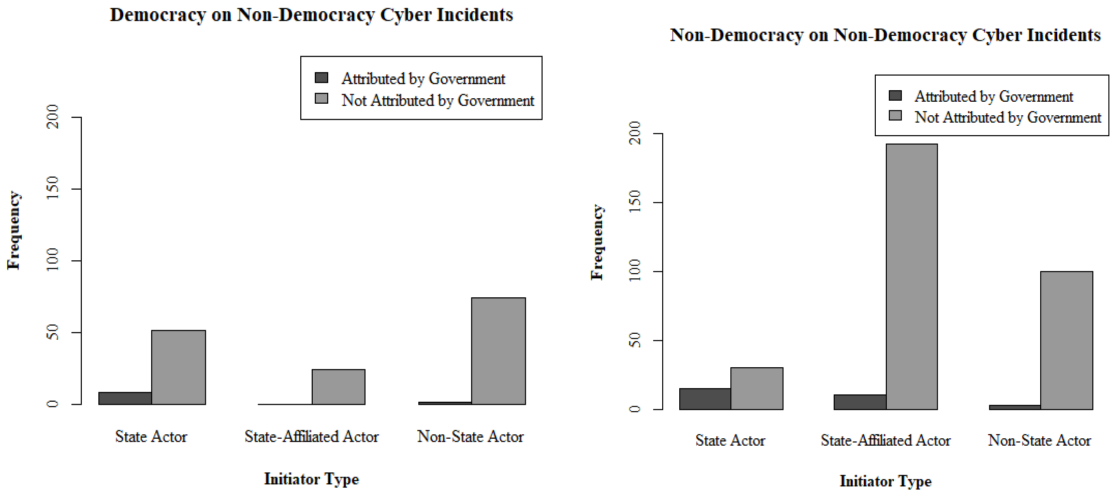
Models 2 and 3 include fixed effects for target country region and incident resolution year

Table 9:
Change in Log Odds of Public Attribution Among Non-Democratic Targets, Non-State-Sponsored Initiators

Model	(1)	(2)	(3)
Initiator Regime Type	-0.798 (1.165)	-65 (92738)	-64 (65683)
Weighted Cyberattack Intensity		-0.627 (22900)	-0.928 (16870)
Percent of Targeted Country with Internet Access		1.332 (1754)	0.052* (0.028)
Target GDP per Capita, in thousands USD		0.4 (4.55)	0.4 (3.46)
Neutrality Agreement			-17.192 (414649)
Defense Agreement			19.115 (176245)
Non-Aggression Agreement			-5.154 (217491)
N	159	159	159
AIC	218	52	58

**p<0.1; **p<0.05; ***p<0.01*
Models 2 and 3 include fixed effects for target country region and incident resolution year

Figure 4:
Frequencies of Known Initiator Regime Type and Initiator State Affiliation, Non-Democratic Targets


Democracy on Non-Democracy Cyber Incidents
Attributed by Government
Not Attributed by Government
Frequency
State Actor
State-Affiliated Actor
Non-State Actor
Initiator Type
Non-Democracy on Non-Democracy Cyber Incidents
Attributed by Government
Not Attributed by Government
Frequency
State Actor
State-Affiliated Actor
Non-State Actor
Initiator Type