Assessing the Political Motivations Behind Ransomware Attacks

Karen Nershi[*] Shelby Grossman[†]

October 7, 2022

Abstract

In recent years, ransomware (a type of cybercrime) has received growing attention as a source of risk to the private sector. Although ransomware attacks have traditionally been viewed as apolitical, recent developments suggest there may be a connection between some groups behind these attacks and the Russian government. In this paper, we test whether the behavior of Russia-based ransomware groups is consistent with Russian political goals by comparing the victims of Russia-based groups to those of groups based outside of Russia. To enable this research, we collected a dataset of over 4,000 victims of ransomware attacks located across 102 countries between May 2019 and May 2022 based on information posted to the dark web. Using this data, we find an increase in the average number of attacks by Russia-based groups in the months before an election across six democratic countries, with no similar increase in attacks by groups based outside of Russia. We also analyze leaked chat logs from a major Russia-based ransomware group; based on our analysis, we argue that the Russian government maintains loose ties with ransomware groups in Russia: groups operate as independent criminal organizations but will occasionally perform favors for the government. In exchange, the government provides these groups with safe harbor from prosecution and gains plausible deniability from groups' actions on the world stage. Thus, this paper provides the first evidence of macro-level connections between Russia-based ransomware groups and the Russian government and suggests the need for more analysis of international security threats emerging from cybercrime.

[*] Postdoctoral Fellow, Stanford Internet Observatory, nershi@stanford.edu.

[†] Research Scholar, Stanford Internet Observatory, shelbybg@stanford.edu.

1 Introduction

Over the last decade, ransomware attacks have presented a major threat to entities in both the public and private sector in countries around the world. These destructive attacks involve the use of malware to encrypt a victim's files, with attackers then demanding a ransom (generally payable in cryptocurrency) in exchange for the decryption key. Although most of these attacks are perpetrated by criminals, the circumstances surrounding some attacks suggest that political motivations and connections to state actors may also play a role. In this paper, we probe for potential ties between ransomware groups and states using newly collected data about the victims of ransomware attacks.

While it is typically difficult to acquire unbiased data about the victims of ransomware attacks due to victims' interest in concealing these attacks to protect their reputations, a recent development in the way criminals perpetrate these attacks has enabled the collection of data directly from criminal groups themselves. Specifically, ransomware groups have turned to a tactic known as "double extortion," which has led many groups to maintain sites on the dark web where they share information about their victims. We leveraged this fact to collect a dasaset of the victims of ransomware attacks.

To enable this research, we identified active ransomware groups that maintained "leak sites" on the dark web and visited these sites regularly between October 2021 and May 2022 to collect information using both automated and manual web scraping. We then harmonized our findings with that of a publicly available dataset provided by a private cyber security company, Dark Tracer. For each victim, we then recorded in which country the victim was located (or headquartered) and the victim's sector according to a standardized industry classification system. In total, our dataset includes information on over 4,000 victims located in 102 countries across 27 sectors between May 2019 and May 2022.

Using this data, we compare the victims of groups based in Russia to the victims of groups based outside of Russia to identify behavior consistent with Russian political goals.

Specifically, we exploit exogeneity around the timing of elections in six major democracies (which have the highest number of ransomware victims of all countries in the sample) and find that the average daily attacks by Russia-based groups increased before elections, with no similar increase in attacks by ransomware groups based outside of Russia. We argue that this trend is consistent with efforts to target election infrastructure before elections and may also be driven by a "spill over" effect from other types of Russian cyber activity before elections, as actors contracted by the Russian government to carry out other types of cyber attacks may use common exploits to deploy ransomware for financial gain. We also test whether Russia-based groups target companies with larger assets on average, which could be indicative of the fact that these groups possess greater resources due to their connections to a state government (Russia); however, we do not find evidence that Russia-based groups target companies with greater assets on average than groups based outside of Russia.

To further assess the relationship between the Russian government and ransomware groups, we analyze qualitative evidence from two years of leaked chat logs from one of the biggest Russia-based ransomware groups, Conti. These logs paint a picture of a group not unlike a Silicon Valley startup, albeit engaged in criminal rather than legal business. Specifically, the group includes employees performing roles ranging from human resources recruiter to trainer to project manager. While much of the groups' work is relatively mundane – including communicating with clients, negotiating payments with affiliates, and researching potential blockchain applications that could be used to launder money – some activity reveals connections to the Russian government. In particular, the FSB (the Russian security service) requested that the group hack a journalistic organization, and Conti's top leaders "patriotically" responded by hacking the organization and sharing its information with the FSB.

Based on analysis of these leaked chat logs and our quantitative results, we argue that the Russian government maintains *loose ties* with ransomware groups in what appears to be a mutually beneficial relationship. Ransomware groups generally operate as independent criminal organizations but will occasionally perform favors for the Russian government; in exchange, the Russian government typically offers these groups safe harbor from prosecution. For the Russian government, this arrangement provides plausible deniability from these groups' actions on the world stage. Thus, our research provides the first evidence of macro-level connections between the actions of Russia-based ransomware groups and Russian political objectives.

Our research contributes to the international security literature on cyber warfare by providing evidence of the need for a broader conception of the international security threats emanating from the cyber realm. While much prior research has focused on national security threats emerging from politically-motivated cyber attacks by state actors, our research suggests that cybercrime *can also* have an international security component and impact a country's national security over the long term. In particular, we highlight the need for a broader conception of the actors involved in politically-linked cyber attacks to include actors that are not directly tied to states, as well as a broader understanding of the mixed political and financial motives that may underlie cyber attacks. Lastly, our research suggests that cyber security scholars should develop a broader conception of the victims and damage caused by cyber attacks, as the traditional viewpoint has largely dismissed damage to the private sector that may occur over a long period of time but produces significant *cumulative costs.*

The rest of the paper is structured as follows: first, we situate our research within the literature and describe our specific contributions. Second, we detail our predictions and third, we describe our newly-collected data. Fourth, we detail our research methods and results, and fifth, we provide concluding thoughts.

2 Actors and Motivations Behind Cyber Attacks

Over the past two decades, a range of actors have employed cyber attacks for a variety of reasons as cyber has emerged as a new domain of state-driven and private competition.

The most common type of cyber threat generally involves attacks by financially-motivated individuals against companies and individuals through scams, fraud, and theft. Some of these schemes are nearly as old as the internet itself, with scammers sharing spam and malicious ads online as well as engaging in social engineering scams such as the now famous "Nigerian Prince" scam (Brunton 2013). As the years have progressed, many of these forms of cybercrime have become more sophisticated, and in recent years, thefts of large amounts of cryptocurrency has emerged as a major threat to cryptocurrency businesses.

Likely less well known, however, is the way that *states* have used cybercrime to earn hundreds of millions and even billions of dollars. North Korea is one of the most notorious offenders, with government-linked hackers carrying out a major heist against Bangladesh's national bank that resulted in the loss of $81 million, which (fortunately) was much less than the intended haul of nearly $1 billion (White and Lee 2021). All told, state-backed hacks against businesses and national banks have allowed North Korea to obtain at least $1.75 billion in illicit funds, according to cryptocurrency analytic firm Chainalysis (White and Lee 2021; Caesar 2021). Iran is another country that has engaged in state-backed cybercrime, with the U.S. Department of Justice (DOJ) indicting individuals connected to Iran's Islamic Revolutionary Guard Corps in 2018 for state-sponsored attacks against governments and companies located around the world (Department of Justice 2018). The Iranian government has also encouraged Bitcoin mining as a way to evade international sanctions (Robinson 2021).

States have also used the cyber realm to advance their political goals, with one of the most famous cases to date involving a virus known as Stuxnet that was likely developed by Israel and the United States; this malware was then deployed against an Iranian government unit engaged in the country's nuclear enrichment program, rendering many of the unit's computers unusable (Lindsay 2013). While Stuxnet highlights the impact that cyber attacks can have on a country's physical structures, states have also used cyber capabilities to complement actions on the ground during conflicts or other politically contentious times.

Table 1: Actors and Motivations in Cyber Attacks

	State Actor	**Non-State Actor**
Financial Motives	North Korean state-backed hackers; Iranian state-backed hackers	Cybercriminals
Political Motives	Stuxnet; Russian cyber attacks against Estonia (2007), Georgia (2008), and Ukraine (2014)	Anonymous

Notably, Russian-backed cyber actors carried out a large-scale attack against Estonia in 2007 following the country's removal of a Soviet-era statue. These attacks knocked many government websites offline along with banking and media sites, disrupting normal activities for many Estonians for nearly a day (McGuinness 2017). Russia has also used similar tactics in Georgia and Ukraine during politically contentious times in both countries.

Lastly, politically-minded non-state actors – known as "hacktivists" for their commitment to social activism through hacking – have also used cyber attacks to achieve their social and political objectives. Likely the best known group in this category is Anonymous, which has used hacking and distributed denial-of-service (DDoS) attacks to target ethically dubious companies like Ashley Madison (an online dating site designed for married individuals seeking an affair) by threatening to release the company's client list if it refused to cease operations (the company did not, and Anonymous leaked the information) (Zetter 2015). More recently, hacktivists have been active on both sides of the Russia-Ukraine conflict, with members of the Ukrainian government issuing a direct call for hackers to "get involved in the cyber defense of [Ukraine]" (Schectman and Bing 2022).

Within this two-way dichotomy of state and non-state actors driven by political or financial motives (see Table 1), ransomware defies easy categorization. On the one hand, attacks have largely been understood as financially motivated, yet on the other hand, attacks in recent years have targeted private and public entities providing critical services including schools, hospitals, and government offices; these attacks call into question the degree to which some attacks may be politically motivated. Further, there is a long-standing geopolitical aspect to ransomware, as many of the groups behind these attacks are located in Russia and Eastern Europe.

Table 2: Malware-Avoiding Keyboard Languages

Language	**Keyboard Number**
Russian	419
Ukrainian	422
Belarusian	423
Tajik	428
Armenian	42B
Azerbaijani (Latin)	42C
Georgian	437
Kazakh	43F
Kyrgyz (Cyrillic)	440
Turkmen	442
Uzbek (Latin)	443
Tatar	444
Romanian (Moldova)	818
Russian (Moldova)	819
Azerbaijani (Cyrillic)	82C
Uzbek (Cyrillic)	843
Arabic (Syria)	2801

Notes: Text taken from Krebs (2021). This table shows a list of keyboard languages that one particular malware strain checked whether a user had installed; if so, the malware exited without running on the machine.

Indeed, Russia and Eastern Europe's prominence in the world of ransomware is a function of both supply – as many former Soviet countries have highly ranked universities that train students in technical skills – and demand – as graduates face few high-paying tech jobs in the private sector, and law enforcement (particularly in Russia) has exerted little effort to prosecute cybercriminals (Maurer 2018). Indeed, Russian authorities have only once arrested ransomware attackers in a move that was widely perceived as an effort to gain leverage over Western countries before Russia's invasion of Ukraine (Dixon and Nakashima 2022; Nechepurenko 2022). In a seeming detente, many Russian-language ransomware groups have refrained from targeting companies in Russia and Russia's broader sphere of influence, with exceptions often written directly into the malware (see Table 2) (Maurer 2018; Krebs 2021). By contrast, other countries (including Eastern European countries like Ukraine) have coordinated criminal investigations internationally leading to the arrests of high-profile individuals involved in ransomware (INTERPOL 2021; DOJ Office of Public Affairs 2021; Miller 2021; Krebs 2022e; DOJ Office of Public Affairs 2021; Toulas 2021; Lakshmanan 2022; Lakshmanan 2021).

Despite the prevalence of destructive ransomware attacks in recent years, ransomware has received relatively little attention from cybersecurity scholars and many policymakers because it has been commonly understood as a form of crime. We seek to remedy this deficiency by exploring the international security dimensions of ransomware attacks, focusing particularly on potential connections between ransomware groups based in Russia and Russia's political objectives. Thus, our research considers a type of cyber attack that appears to fall somewhere near the middle of Table 1, characterized by financial and potentially political motivations and perpetrated by non-state actors with ties to a state government.

2.1 Broadening Conceptions of Cyberwarfare

Our research contributes to the international security literature on cyber warfare by broadening the empirical and theoretical understanding of cyber threats. Over the last twenty years, a robust body of scholarship has explored cyber technology as it relates to international security concerns. Scholars have considered whether cyber primarily advantages offensive or defensive military capabilities (Lindsay and Gartzke 2016; Gartzke 2013; Gartzke and Lindsay 2015), whether cyber constitutes a new strategic military domain or merely augments existing domains (Lindsay and Gartzke 2016; Lindsay and Gartzke 2020), whether cyber is useful for coercion or deterrence (Lindsay and Gartzke 2016; Borghard and Lonergan 2017; Borghard and Lonergan 2021; Gartzke, Lindsay, and Nacht 2014), and questions of signaling and credible threats related to the cyber domain (Lonergan and Lonergan 2022).

While these accounts have made significant progress in analyzing cyber capabilities within the context of war and warfighting, we argue that the emphasis placed on traditional military capabilities has led scholars to overlook an important vector of international security threats emerging from the cyber domain: that of cybercrime and ransomware in particular. Thus, we argue that developments on the ground call for a broader conceptual framework through which to analyze cyber security threats, particularly along three dimensions – the actors involved, their intentions, and the nature of damage resulting from these attacks.

First, our research seeks to broaden conceptions of the types of actors that may present international security risk to include non-state actors without direct ties to states. Most cybersecurity research thus far has distinguished between state actors and non-state actors, and typically dismissed the latter as inconsequential for international security. For example, some argue that because greater resources and capabilities are necessary to carry out an impactful cybersecurity attack, attacks by non-state actors are generally inconsequential (Lindsay and Gartzke 2016; Ashraf 2021). Yet increasingly, real-world evidence suggests that these lines, especially in the context of Russia's engagement with cyber actors, are often blurred. For example, in the ongoing conflict between Russia and Ukraine, security firm Mandiant has uncovered links that suggest coordination between pro-Russian hackers and Russian military intelligence (the GRU) in attacks carried out against Western government offices and defense contractors (McMillan and Volz 2022). Along with this emerging evidence, our research supports the case for broadening conceptions of potential politically-linked cyber actors to include criminals and other actors that may not be directly tied to a state.

Second, our research highlights the potential for mixed financial and political motives by cyber actors. In a similar vein, most past accounts have sought to distinguish between political and financial motives behind attacks, typically regarding the first as a potential threat to international security and the latter as a minimally-harmful "irritant" or "nuisance" (Lindsay and Gartzke 2016; Gartzke and Lindsay 2015; Rid 2012; Solis 2014; Cornish et al. 2010). Our research highlights that in practice, drawing this distinction is often more ambiguous, and in fact, mixed financial and political motives have been identified in several major cyber attacks, including an FSB-led hack of Yahoo in 2014 (Department of Justice 2017). Dividing political and financial motives also becomes complicated in the context of China's widespread espionage against U.S. and other Western companies; the Chinese government is often behind efforts that then benefit Chinese businesses, which themselves straddle both public and private interests as many are closely aligned with the government and the Chinese Communist Party. Thus, both the Chinese government and the private sector more broadly benefit from cyber espionage (Wray 2020).

Third, our research seeks to broaden notions of the nature of victims and damage resulting from cyber attacks. Because much of the research has focused on the context of warfare, scholars have generally placed a high threshold for the types of cyber attacks that should merit attention, focusing primarily on the risks of a singular disruptive attack. For example, in an an early and influential article, Rid (2012) argues that cyber warfare must involve a lethal attack; otherwise, he argues, an attack presents a lesser form of cyber meddling such as sabotage, espionage, or subversion. Later, scholars allowed for a broader conception of the repercussions of cyber attacks to include "damage" – such as harm to physical structures rather than solely the loss of human life (Stone 2013). In the literature's broadest definition, scholars have considered threats to critical infrastructure as a potential cyber risk. Even these conceptions are still somewhat conservative, however, focusing on attacks that cause significant harm in the real world, such as an attack against an air traffic control network that results in the crash of a civilian airline (Solis 2014; Tsagourias 2012).

Further, much of the literature has focused on the risks of a singular, highly disruptive cyber attack. This inclination is also present amongst some in the public sector, with Defense Secretary Leon E. Panetta warning in 2012 of the risk of a "cyber-Pearl Harbor" that could devastate the national electric grid, the supply of clean water, or a major transportation network (Bumiller and Shanker 2012). Importantly, this focus on the risk of a single major attack has been largely derived by scholars' interest in the type of cyber attack that might prove decisive during war or precipitate the start of a new war, as the Pearl Harbor reference makes clear. Although it is important to consider the risk of a major cyber attack that could result in loss of life or draw the country into a war, we argue that this emphasis has led scholars to overlook an imminent cyber security threat that the U.S. and other Western countries already face – that of significant cumulative costs inflicted on the private sector through a series of small-scale attacks perpetrated over a period of months and years (rather than hours or days).

Indeed, over a decade ago, National Security Agency Chief General Keith Alexander stated that cybercrime had resulted in the "greatest transfer of wealth in history" (Rogin 2012). The costs of cybercrime have only increased over time, with the Federal Bureau of Investigation (FBI) estimating that cybercrime led U.S. businesses to lost $6.9 billion in 2021 alone (Federal Bureau of Investigation 2022, p. 3). Because of the nature of these costs, however, which are primarily borne by the private sector and spread out over time, they have attracted less attention than politically motivated cyber attacks. Thus, we argue for the need to adopt a broader conceptual framework of the types of international security risks emerging from the cyber realm to include risks from cybercrime.

Beyond broadening conceptions of cyber security threats, our research contributes to ongoing discussions around the challenge of attribution in state cyber competition. Specifically, much of the early work argues that the difficulty of attributing cyber actions to the actors behind them renders cyber an offense-dominant space (Clark and Landau 2011; Libicki 2009), with work focusing on both the technical and legal challenges of attribution (Rid and Buchanan 2015; Tsagourias 2012; Egloff and Smeets 2021). Others argue that attribution may not prove such a challenging task after all, as only certain actors possess the capabilities necessary to carry out sophisticated cyber attacks (thus narrowing the list of potential suspects) (Lindsay 2013); However, attribution becomes decidedly more complicated when one considers cases of mixed political and financial motives.

Accordingly, the potential for mixed motives suggests that the accurate attribution of cyber attacks may require greater time and resources than previously recognized. In particular, the fact that cyber actors like ransomware groups may choose to engage in high-volume yet relatively small-scale attacks suggests that actors' capabilities are unlikely to play an important role in determining attribution for smaller-scale attacks, though these attacks can still have an important impact in the aggregate. Specifically, in the case of Russia, we argue that this mixing of financial and political motives is part of a deliberate strategy to create ambiguity about the government's intentions and actions, which allows the state to maintain "plausible deniability" on the world stage from these groups' actions.

Finally, our research contributes to the existing literature by providing analysis of systematic data for one particular type of cyber attack. Indeed, a systematic review of the literature argues that research on cyber warfare has often been theoretical and placed less emphasis on empirical results (Gorwa and Smeets 2019). This is partly explained by the fact that obtaining information about cyber attacks can be challenging for a number of reasons, including the fact that victims (whether governments offices or private companies) often have an incentive to keep an attack private to avoid potential reputational harm. Thus, our research contributes to the literature on cyber warfare by providing analysis of systematic data about ransomware attacks.

3 Predictions

3.1 Attacks Against Wealthier Targets

First, we predict that the victims of ransomware attacks by Russia-based groups will likely have greater assets than the victims of attacks by non-Russia-based groups. Importantly, greater resources are necessary to carry out attacks against larger targets, which in turn have allowed groups to demand larger average ransoms. Thus, we form this prediction under the assumption that Russia-based groups may have connections to the Russian government that provide them with greater resources, allowing them to carry out more sophisticated attacks against wealthier victims than ransomware groups based outside of Russia, which presumably do not have connections to a state government.

3.2 Increased Attacks Before Elections

Second, we predict that attacks by Russia-based groups will increase before elections in Western democracies. Preliminary evidence suggests ransomware attacks may pose a threat to elections in democracies, and this was a major concern expressed by the U.S. government before the 2020 U.S. presidential election (Bing 2019; Marks 2019). If attacks by Russia-based groups increase before elections, this would suggest the existence of a connection between the targeting choices of Russia-based ransomware groups and the Russian government's political objectives.

One potential alternative explanation for this relationship is that ransomware groups are able to more successfully extort ransoms in the periods before elections, incentivizing an increase in attacks. For example, if victims are more willing to pay a ransom in the weeks before an election to ensure their systems will be up and running, this could lead ransomware groups to increase attacks before elections for financial reasons. To assess the plausibility of this potential alternative explanation, we compare the average number of attacks by groups based within and outside of Russia before elections. Accordingly, if financial reasons primarily drive an increase in attacks, then we should not expect to see a significant difference in the targeting patterns of both types of groups.

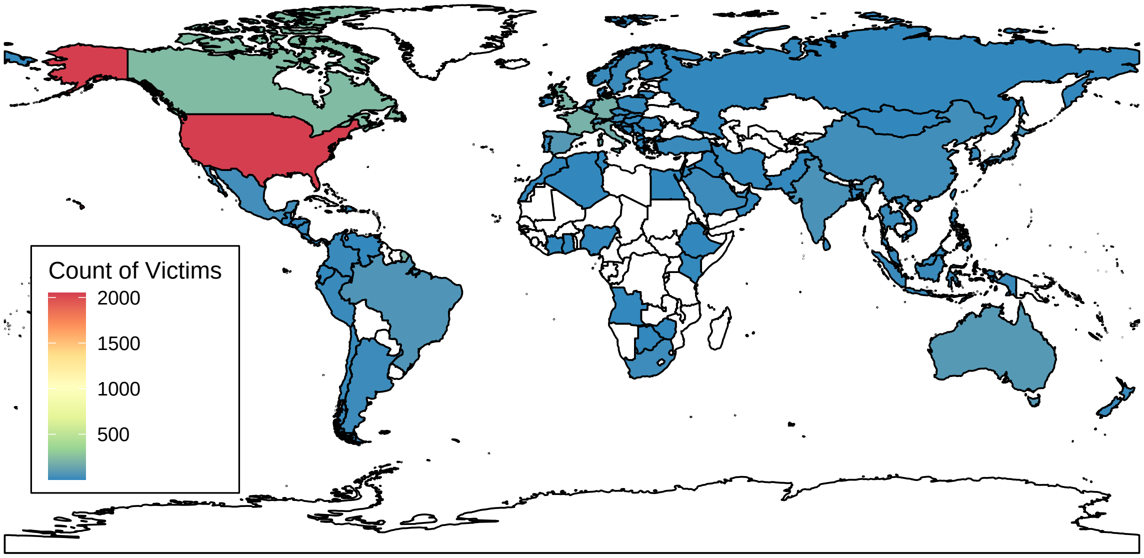
4 Data

One of the chief challenges in studying cyber intrusions lies in obtaining reliable data about these events (Gorwa and Smeets 2019). In the case of ransomware attacks, for example, victims have an incentive not to disclose information about a breach since such a disclosure could bring legal liability and reputational harm. To address this challenge, we collected data directly from ransomware groups themselves via sites on the dark web. Specifically, we collected information on the victim and date of each attack from ransomware groups that carry out so-called "double extortion" attacks, leading them to maintain sites on the dark web where they share information about each victim.

Our dataset includes 4,194 ransomware victims between May 1, 2019 and May 1, 2022. Of these, 2,254 victims were identified from the Dark Tracer dataset, 1,519 were identified through our dataset, and 421 victims were included in both datasets. The data includes victims attributed to 55 unique ransomware groups; of these, 8 are Russia-based groups, and the remaining 47 are based elsewhere or have no known origin. Russia-based groups carried out attacks against 1,910 victims (45.5%), while non-Russia-based groups carried out attacks against 2,284 victims (55.5%). For each victim, we identified in which country the business was located or headquartered and its sector. The victims of these attacks were located across 102 countries, although over half of all victims were located in the United States (see Figure 1).

Table 3 presents summary statistics for the percent of victims by country for non-Russia-based and Russia-based groups. The data show that Russia-based groups target a higher percentage of victims in the United States than non-Russia-based groups (58.9 versus 45.0

Figure 1: Victim Count by Country



Notes: Heat map shows the number of victims of ransomware attacks within our dataset by country.

Table 3: Victims by Country: Russia vs. Non-Russia-based Groups

Country	Percent of Victims		
	Russia-Based Groups	*All Other Groups*	Chi-Squared Test
USA	58.9	45.0	76.29***
Canada	6.1	5.5	0.73
France	4.2	5.3	2.17
Italy	3.3	4.8	4.73*
Germany	5.2	4.1	2.37
United Kingdom	6.4	3.8	13.68***
All other countries	22.3	35.3	133.49***
N	1,910	2,284	

Notes: Columns (1) and (2) show the proportion of victims by non-Russia-based and Russia-based groups from each country. Column (3) shows the X^2 value of a Chi-squared test; *p < .05; **p < .01; ***p < .001.

percent), a difference that is statistically significant based on a Chi-squared test comparing the two distributions ($p < 0.001$). Russia-based group also target a higher percentage of victims in the UK (6.4% versus 3.8%), which is statistically significant ($p < 0.001$). On the other hand, Russia-based groups are *less likely* to target victims in Italy (a difference of 1.5 percentage points, $p < 0.05$). Lastly, Russia-based groups are *less likely* to target victims located in *any other country than those with the top six number of victims* (the United States, Canada, France, Italy, Germany, and the United Kingdom) by a difference of 13 percentage points, and this difference is statistically significant ($p < 0.001$).

We also compare the victims of Russia-based and non-Russia-based groups by sector. Table 4 shows the percentage of all victims that fall into one of fourteen sectors For most sectors, there is little difference between the percentage of victims by Russia-based and non-Russia-based groups, as evidenced by the χ^2 values in column 3. However, Russia-based groups have a higher percentage of victims in the education and public administration

Table 4: Victims by Sector: Russia vs. Non-Russia-based Groups

Country	Percent of Victims		Chi-Squared Test
	Russia-Based	*All Others*	
Industrials	27.0	27.0	0.00
Consumer Discretionary	15.8	15.1	0.34
Other Services	8.6	9.3	4.9
Information Technology	6.3	8.1	4.54*
Materials	7.9	7.4	0.30
Financials	4.5	6.7	8.05**
Health Care	6.2	6.3	0.001
Consumer Staples	5.4	4.4	1.84
Pubic Administration	4.6	3.6	5.26*
Education	5.0	2.7	13.72***
Communication Services	2.6	3.1	0.71
Real Estate	2.5	2.5	0.00
Energy	2.0	1.9	0.01
Utilities	1.6	1.9	0.46
N	1,910	2,284	

Notes: Columns (1) and (2) show the proportion of victims by non-Russia-based and Russia-based groups by sector. Column (3) shows the X^2 value of a Chi-squared test; *p < .05; **p < .01; ***p < .001.

sectors, differences that are statistically significant based on the results of a Chi-squared test. Russia-based groups also have a lower percentage of victims in the information technology and financial sectors than non-Russia-based groups, which are statistically significant.

5 Results

5.1 Attacks by company size

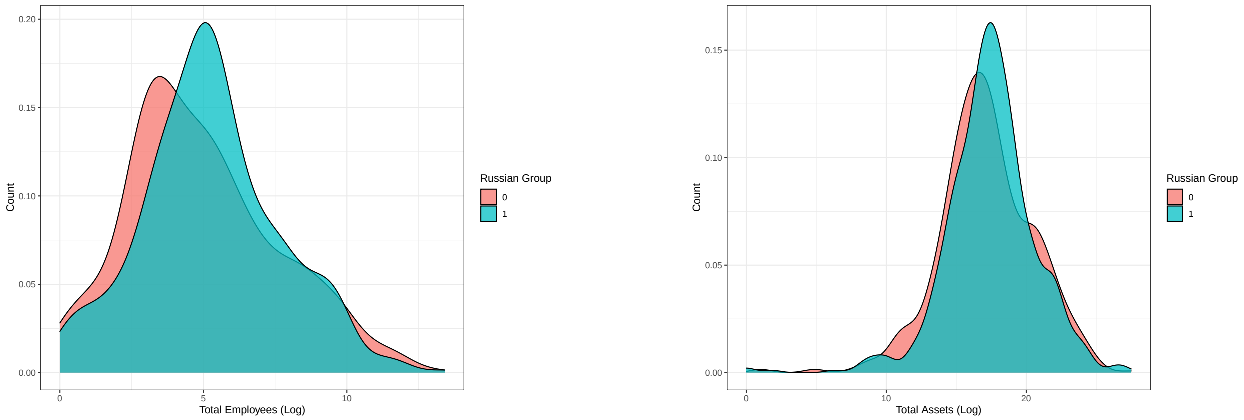
To test whether Russia-based groups target larger companies on average, we matched victims with company data, obtaining 1,309 matches (31% of the total dataset). The matched data includes information about 705 victims of 30 non-Russia-based groups and 604 victims of 9 Russia-based groups. We consider two characteristics of companies which we chose in part based on their prevalence within the data: a company's number of employees and a company's total assets (in dollars). Histograms in Figure 2 show the distribution of the logged count of employees (2a) and logged total assets (2b) for victims of all Russia-based and non-Russia-based groups. While there is little difference in the means of the logged total assets for victims of these two types of groups, the average logged count of employees is slightly higher for Russia-based groups, a difference that is statistically significant based on a one-sided t-test of the means ($p < 0.05$) (see Table 5, row 1).

Table 5: Russia vs. Non-Russia-Based Groups

	Total Assets (Logged)			**Employees (Logged)**		
	Non-Russia-Based	Russia-Based	Difference	Non-Russia-Based	Russia-Based	Difference
Mean	17.07	17.26	0.19	5.02	5.31	0.29*
	(3.57)	(3.60)	(0.20)	(2.56)	(2.33)	(0.14)
Mean by Group	17.03	17.26	0.23	5.00	5.45	0.43
	(1.75)	(0.90)	(0.60)	(1.29)	(0.58)	(0.44)

In addition, we consider whether characteristics vary significantly between Russia-based and non-Russia-based groups when characteristics are measured at the group level. Figure 3 shows the difference in the average logged count of employees by group (3a) and the average

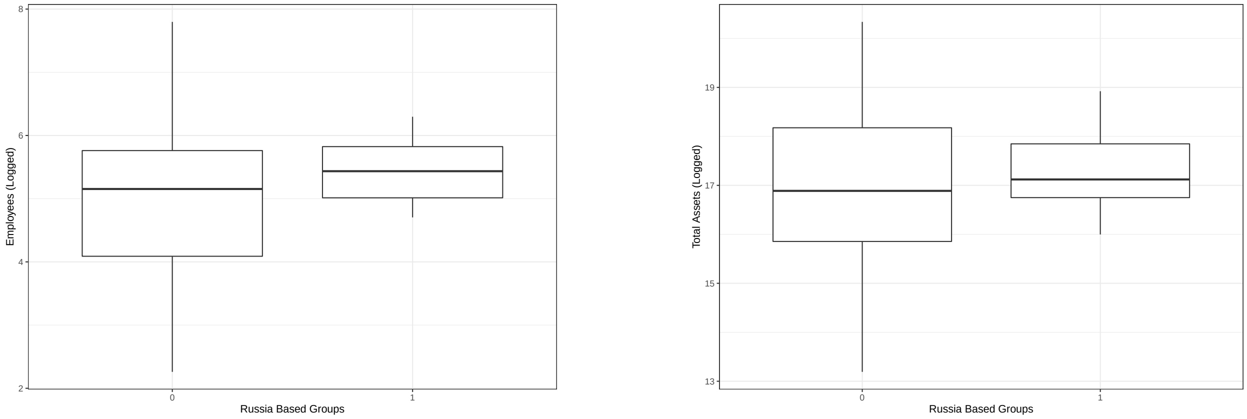
Figure 2: Company Characteristics Across All Victims



(a) Employees (Logged)

(b) Total Assets (Logged)

Figure 3: Average Group-Level Characteristics



(a) Employees (Logged) by Group

(b) Total Assets (Logged) by Group

logged total assets by group (3b) between Russia-based and non-Russia-based groups. These plots show that there is little difference in the average mean for both types of groups across both variables, and, indeed, the difference in means by groups for these characteristics is not statistically significant (see Table 5, row 3).

Lastly, we run a regression model to test whether the relationship between Russia-based groups and a victim's logged total assets is statistically significant after controlling for several relevant factors. Table 6 shows the results of these models after controlling for group, month-year, and sector fixed effects. Although there is a positive relationship between Russia-based groups and the log of a company's total assets, it is not statistically significant. We run a model with the same specification to test the relationship between Russia-based groups and the a company's logged employee count. Once again, we find that there is no statistically significant relationship between Russia-based groups and a victim's employee count after controlling for group, month, and sector fixed effects (column 2 of Table 6).

Table 6: Regression of Victims' Total Assets and Number of Employees

	Total Assets (Logged)	*Employees (Logged)*
	(1)	(2)
Russian	2.180	−0.384
	(1.634)	(1.627)
Constant	13.846***	5.277**
	(2.082)	(1.930)
Group FEs	✓	✓
Month-Year FEs	✓	✓
Sector FEs	✓	✓
Observations	1,230	1,031
R^2	0.124	0.136
Adjusted R^2	0.058	0.057

Note: *p<0.05; **p<0.01; ***p<0.001

In short, these results show *no statistically significant relationship* between the size of a victim's total assets or employees and Russia-based groups. Stated another way, Russia-based groups do not appear to target companies with larger total assets or employee counts than non-Russia-based groups. However, these results should be interpreted with caution given the non-random nature of matching victims with company-level characteristics. Specifically, we cannot conclude that the proportion of our sample that we managed to match with company data represents a random sample of our underlying dataset. Accordingly, there could be a type of systematic bias that underlies the matches we obtained. However, based on the data we have, these results suggest that Russia-based groups do not target larger companies on average than non-Russia-based groups.

5.2 Attacks by Russia-based groups before elections

We also test whether attacks by Russia-based groups increase before elections. Between February 1, 2020 and April 30, 2022, Canada and Germany held federal elections, the United States, Italy, and France held presidential elections (Table 7); the United Kingdom did not hold national-level elections during this period.

Table 7: National Elections

USA	Presidential Election	November 3, 2020
Canada	Federal Election	September 20, 2021
Germany	Federal Election	September 26, 2021
Italy	Presidential Election	January 24, 2022
France	Presidential Election	April 24, 2022

We find an *increase* in the number attacks by Russia-based groups in the three months preceding elections for the six democratic countries in our sample (Table 8), where the dependent variable is the number of attacks by a Russia-based group in a country on a given day. We find there is a 26.6 percent increase in the chances of an attack by a Russia-based group on a given day one month before an election. Two months before an election, there is a 41.1 percent increased chance of an attack on a given day, and there is a 41.6 percent increased chance in the three months before an election.

Similarly, we test whether there is an increase in the number of attacks by *non-Russia-based groups* before elections, with the results presented in Table 9. Once again, the dependent variable is the number of ransomware attacks on a given day during the one, two, or three month periods before an election for each of the six countries with the most ransomware attacks. However, unlike for Russia-based groups, there is no statistically significant relationships between the period before an election and the number of ransomware attacks by

Table 8: Attacks by Russia-Based Groups Before Elections

	Number of attacks		
	(1)	(2)	(3)
One month	0.266**		
	(0.096)		
Two months		0.410***	
		(0.083)	
Three months			0.416**
			(0.134)
Germany	−0.017	−0.017	−0.017
	(0.022)	(0.022)	(0.022)
France	−0.027	−0.006	0.010
	(0.021)	(0.022)	(0.026)
United Kingdom	0.015	0.035	0.051$^{\cdot}$
	(0.025)	(0.026)	(0.029)
Italy	−0.057**	−0.057**	−0.057**
	(0.019)	(0.019)	(0.020)
USA	1.126***	1.126***	1.126***
	(0.081)	(0.081)	(0.081)
Constant	−0.145***	−0.151***	−0.157***
	(0.037)	(0.037)	(0.038)
Month-Year FEs	✓	✓	✓
N	4,914	4,914	4,914
R^2	0.182	0.186	0.189
Adjusted R^2	0.177	0.181	0.184

Notes: The unit of observation is the country-day for the top six countries with ransomware attacks – the USA, Canada, United Kingdom, France, Germany, and and Italy. Robust standard errors are clustered at the country level; *p < .05; **p < .01; ***p < .001.

non-Russia-based groups.

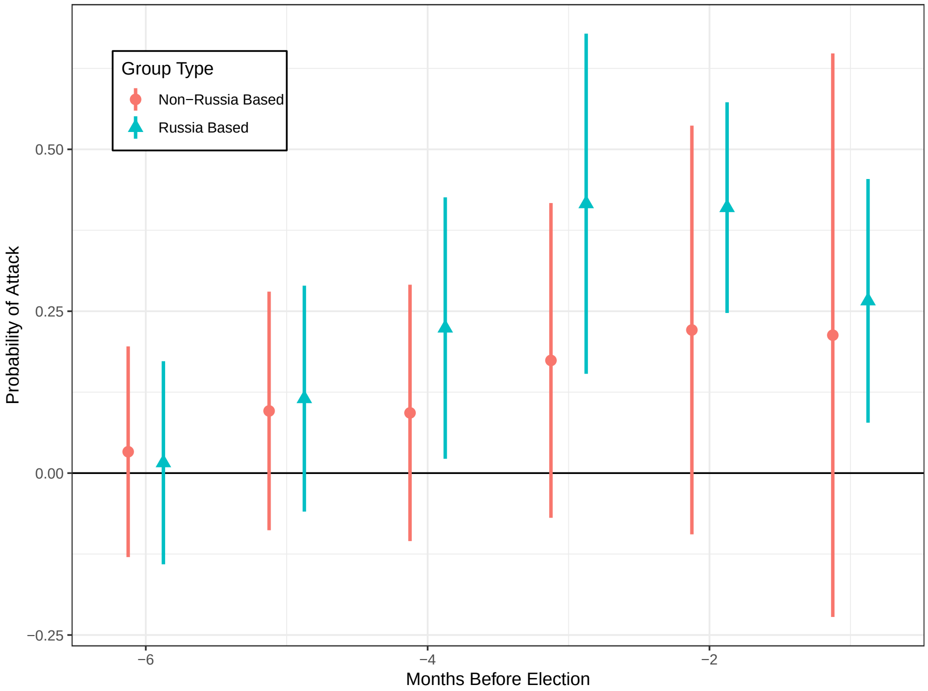
Table 9: Attacks by Non-Russia-Based Groups Before Elections

	Number of attacks		
	(1)	(2)	(3)
One month	0.213		
	(0.222)		
Two months		0.221	
		(0.161)	
Three months			0.174
			(0.124)
Germany	-0.043^{*}	-0.043^{*}	-0.043^{*}
	(0.020)	(0.020)	(0.020)
France	−0.005	0.003	0.006
	(0.024)	(0.026)	(0.027)
United Kingdom	$-0.037^{\cdot}$	−0.029	−0.026
	(0.021)	(0.023)	(0.024)
Italy	−0.018	−0.018	−0.018
	(0.021)	(0.021)	(0.021)
USA	0.991^{***}	0.991^{***}	0.991^{***}
	(0.077)	(0.076)	(0.076)
Constant	-0.108^{**}	-0.111^{**}	-0.112^{**}
	(0.033)	(0.034)	(0.034)
Month-Year FEs	✓	✓	✓
N	4,914	4,914	4,914
R^2	0.158	0.158	0.158
Adjusted R^2	0.152	0.153	0.153

Notes: The unit of observation is the country-day for the top six countries with ransomware attacks – the USA, Canada, United Kingdom, France, Germany, and and Italy. Robust standard errors are clustered at the country level; *p < .05; **p < .01; ***p < .001.

To further probe this relationship, we estimate the daily number of attacks by Russia-based and non-Russia-based groups across longer time horizons. Figure 4 shows coefficients for the full model (including month-year and country fixed effects) for both Russia and non-Russia-based groups in the periods leading up to an election. The graph shows there

Figure 4: Attacks by Russia-Based and non-Russia-Based Groups in Months Before Elections



Notes: Plot shows coefficients for the full models (including month-year and country fixed effects) for the likelihood of an attack on a given day in the period before an election within six democracies – the USA, Canada, United Kingdom, France, Germany, and Italy.

is no statistically significant difference between the likelihood of an attack by a Russia-based or non-Russia-based group in the five and six months before an election for the six democracies we consider. However, there is an increase in the likelihood of an attack by a Russia-based group in the four months before an election, and this likelihood increases and remains statistically significant in the three, two, and one month periods before an election. We see no similar increased in the likelihood of an attack by non-Russia-based groups. These findings suggest while Russia-based groups appear to operate in similarly to non-Russia-based groups in earlier periods, their behavior changes as elections near as these Russia-based groups begin to more actively target victims in the country holding an election.

5.3 Robustness Check

As a robustness check, we also test whether there is an increase in the likelihood of an attack by Russia-based groups in the period before an election when the dependent variable is coded as a binary indicator that is equal to one if there was *at least one ransomware attack on a given day* and otherwise is equal to zero. Similar to the previous specification, we find a positive and statistically significant relationship between the one, two, and three month periods before an election in a country and the chances of at least one attack by a Russia-based group on a given day, although the magnitudes are smaller (see Table 10).

We also use the same specification of the dependent variable to test whether there is an increase in the chances of a ransomware attack in the months preceding an election for non-Russia-based groups. Once again, there is no statistically significant relationship between the number of ransomware attacks and the one, two, and three month periods before an election for non-Russia-based groups (Table 11).

5.4 Why do attacks increase before elections?

There are at least three potential explanations for why Russia-based ransomware groups increase attacks before elections in democracies, which may operate in conjunction with one another or separately.

5.4.1 Damaging election infrastructure

One potential explanation for the increase in attacks by Russia-based groups before elections is that these groups are targeting key election infrastructure in an effort to weaken Western countries and their ability to hold free and fair elections. This was a major concern raised by U.S. cybersecurity and election security officials in the lead-up to the 2020 presidential election (Bing 2019; Marks 2019), with several major ransomware attacks against state and local targets before elections stoking these fears. For example, a mere four weeks before

Table 10: At Least One Attack by Russia-Based Groups

	At least one attack		
	(1)	(2)	(3)
One month	0.069*		
	(0.033)		
Two months		0.102***	
		(0.025)	
Three months			0.093***
			(0.021)
Germany	−0.009	−0.009	−0.009
	(0.015)	(0.015)	(0.015)
France	−0.030*	−0.025$^{\cdot}$	−0.023
	(0.014)	(0.014)	(0.014)
United Kingdom	−0.006	−0.001	0.002
	(0.015)	(0.015)	(0.015)
Italy	−0.040**	−0.040**	−0.040**
	(0.014)	(0.014)	(0.014)
USA	0.376***	0.376***	0.376***
	(0.019)	(0.019)	(0.019)
Constant	−0.026	−0.027	−0.028$^{\cdot}$
	(0.017)	(0.017)	(0.017)
Month-Year FEs	✓	✓	✓
N	4,914	4,914	4,914
R^2	0.225	0.227	0.228
Adjusted R^2	0.220	0.222	0.223

Notes: The unit of observation is the country-day for the top six countries with ransomware attacks – the USA, Canada, United Kingdom, France, Germany, and and Italy. Robust standard errors are clustered at the country level; *p < .05; **p < .01; ***p < .001.

Table 11: At Least One Attack by non-Russia-Based Groups

	At least one attack		
	(1)	(2)	(3)
One month	0.045		
	(0.039)		
Two months		0.026	
		(0.028)	
Three months			0.009
			(0.023)
Germany	$-0.026^{\cdot}$	$-0.026^{\cdot}$	$-0.026^{\cdot}$
	(0.014)	(0.014)	(0.014)
France	-0.017	-0.016	-0.017
	(0.015)	(0.015)	(0.015)
United Kingdom	$-0.024^{\cdot}$	-0.024	$-0.025^{\cdot}$
	(0.015)	(0.015)	(0.015)
Italy	-0.010	-0.010	-0.010
	(0.015)	(0.015)	(0.015)
USA	0.371^{***}	0.371^{***}	0.371^{***}
	(0.020)	(0.020)	(0.020)
Constant	-0.009	-0.009	-0.009
	(0.018)	(0.018)	(0.018)
N	4,914	4,914	4,914
R^2	0.196	0.196	0.195
Adjusted R^2	0.190	0.190	0.190

Notes: The unit of observation is the country-day for the top six countries with ransomware attacks – the USA, Canada, United Kingdom, France, Germany, and and Italy. Robust standard errors are clustered at the country level; $^{*}p < .05$; $^{**}p < .01$; $^{***}p < .001$.

the 2020 U.S. presidential election, a Georgia county suffered a ransomware attack that disrupted access to a voter signature database in addition to other county functions (Fung 2020). In Oregon and Texas, ransomware attackers targeted firms that provide election-related software in the weeks before Oregon's primary and the U.S. 2020 presidential election respectively (Selesky 2022; Perlroth and Sanger 2020). However, perhaps the most serious threat to an election occurred in Louisiana in two apparently unrelated ransomware attacks.

A few hours after Louisiana's election for governor, legislative seats, and other statewide offices in November 2019, a ransomware attack brought down 10% of the state's computer servers, including computers at the Secretary of State's office (though this did not interfere with the state's tally or certification of votes) (Ballard 2019; Bing and Satter 2019). This attack followed an earlier one that came to light only months later, in which a ransomware group breached a contractor for the state via third-party software, which allowed the attackers to access servers across half a dozen parishes (equivalent to counties). One notable aspect of this attack is that even though they had acquired access to state computers four months earlier, the attackers waited until six days before the election to launch their attack (Mehrotra 2020). And while this attack did not disrupt the state's elections, it put significant stress on state and local government offices that facilitated the election.

Even if an attack does not meaningfully affect election results, it can still undermine confidence in election results as part of a "perception hack." Indeed, even a small-scale attack against election infrastructure could lead to widespread distrust in election results. Attackers might, for example, target voting infrastructure in a swing state during a U.S. presidential election, which could reasonably raise doubts about election outcomes at a national level in a close election (Perlroth and Sanger 2020). In fact, an FBI bulletin issued one month before the 2020 U.S. presidential election specifically mentioned this type of risk, cautioning that election-related misinformation could include cyber attacks intended to "convince the public of the election's illegitimacy" (Perlroth and Sanger 2020).

Importantly, this is far from an abstract threat, as Russia has used similar efforts to influence public perception of election results (Perlroth and Sanger 2020). Before Ukraine's 2014 presidential election, for example, pro-Russian hackers infiltrated Ukraine's computer systems and installed malware that led the state's election software to show a far-right candidate had won the election with 37% of the vote, when in reality, the candidate received only 1% of the vote; Ukrainian officials discovered and removed the malware from their system less than an hour before Ukrainian journalists reported the official election results live on television, narrowly avoiding a potential political crisis (Clayton 2014).

However, perhaps the most convincing evidence of ransomware as a major threat to election security came during the lead-up to the 2020 U.S. presidential election. Only weeks before the election, Microsoft and the U.S. Cyber Command worked to neutralize Trickbot, a network of secretly hijacked computers that can be used to distribute malware like ransomware, in parallel but separate efforts (Sanger and Perlroth 2020). And while these measures did not present a permanent solution, Microsoft and the U.S. Cyber Command did manage to disrupt the actions of Russian-speaking cybercriminals in the short term, highlighting the significance both actors placed on ransomware as a potential disrupter of the 2020 election (Sanger and Perlroth 2020).

5.4.2 Creating chaos

A second potential explanation for the increase in attacks by Russia-based ransomware groups is that these attacks are part of broader effort by Russia to create chaos and sow confusion during a politically sensitive time for adversary countries. This explanation matches Russia's strategy in other domains, including state-backed media platforms (Elswah and Howard 2020). One good example of this strategy played out during the lead-up to the 2016 U.S. presidential election, when Russian-backed actors operating on social media platforms fomented discontent on both sides of divisive social issues as part of a broader strategy aimed at creating social unrest and division (Rosenberg, Perlroth, and Sanger 2020; Select Committee on Intelligence United States Senate 2020). It is also worth noting that Russia's goals for employing this strategy may vary. For example, the Mueller Report states that a key goal behind Russia's interference in the U.S. 2016 election was to embarrass and weaken the front-runner domestically rather than to prevent her election altogether (Mueller et al. 2019).

5.4.3 Spillover effect from other Russian cyber attacks

A third potential explanation for the increase in ransomware attacks by Russia-based groups before elections centers on a "spill over" explanation of Russian cybercriminal activity. In particular, the Russian government has commissioned other types of cyber attacks before elections, and if many of the same actors are involved in both cyber attacks for the Russian government and cybercrime, ransomware attacks could increase before elections for a reason unrelated to the Russian government's desire to target Western democracies before elections. Specifically, attacks may increase because actors repurpose cyber exploits generated for official government business to carry out ransomware attacks in their free time. Importantly, while this explanation does not imply an *instrumental* motive behind the increase in ransomware attacks before elections, it does imply close ties between the Russian government and ransomware groups. This explanation rests on several causal links, which I discuss below.

First, this explanation rests on the fact that the Russian government has commissioned other types of cyber attacks before elections in Western countries. One of the most famous such cases was an attack against the Democratic National Committee in 2016, during which a group linked to Russia's FSB hacked the committee's email server; the hackers later leaked the documents through Wiki Leaks in an effort to embarrass the party and its candidate, Secretary Hillary Clinton (Barnes 2020). The same group was later implicated in an attack during the French presidential campaign one year later, in which hackers sought to access and disclose sensitive campaign emails to embarrass the incumbent presidential candidate, Emmanuel Macron (Auchard 2017).

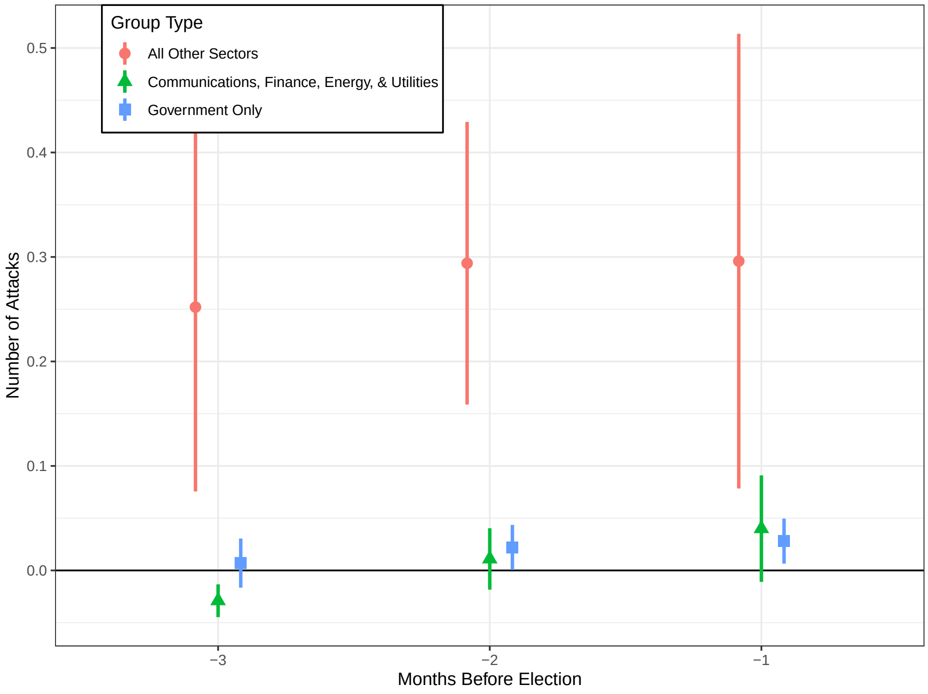
Importantly, carrying out these types of cyber attacks requires actors to develop new "exploits" through which they can gain access to a victim's servers. This could involve deploying large-scale phishing campaigns aimed at luring unsuspecting victims into clicking a link, or discovering a new software vulnerability that enables access to a victim's computer system. Regardless of the method used, many of these cyber exploits could be reused to carry out ransomware attacks (i.e., assuming software developers had not yet issued a patch for a known vulnerability, etc.). Thus, if many of the same actors work for the Kremlin *and* deploy ransomware, then their "work" in one domain could be used as a vector of attack for ransomware.

Indeed, links between Russian government employees and cybercriminals have been established on multiple occasions. For example, two cybercriminals and an FSB agent carried out a major breach against Yahoo, allowing the criminals to benefit financially while the government gained access to information about spies and dissidents. The U.S. government also uncovered that the leader of a major Russian cybercrime group had, in fact, worked with the FSB (Sanger and Perlroth 2020). Thus, it is plausible that some of the actors involved in carrying out cyber attacks for the Russian government may also "moonlight" as cybercriminals, including by carrying out ransomware attacks.

5.5 Plausibility Test

To probe the plausibility of these potential explanations, we look at variation in the sector targeted by Russia-based groups before elections. To test the first hypothesis focused on damage to election infrastructure, we look at attacks against government targets, as state and local governments are the primary actors holding elections. To test whether these attacks might be part of an effort to create chaos, we look at attacks against the finance and media sectors (two of the primary sectors targeted during the 2007 cyberattacks in Estonia) as well as attacks against the energy and utilities sectors, as commentators have specifically noted these sectors as potential targets for ransowmare attacks that could create chaos and impede

Figure 5: Attacks by Russia-Based Groups by Sector in the Months Before Elections



Notes: Plot shows coefficients for the full models (including month-year and country fixed effects) for the number of daily attacks by Russia-based groups across there types of targets – targets in the government sector; targets in the communications, finance, energy and utilities sectors; and victims in all other sectors *except for* the government, communications, finance, energy and utilities sectors – during the one, two, and three month periods before an election across six democracies: the United States, Canada, United Kingdom, France, Germany, and Italy.

a national election (Stahl 2020). Lastly, to test a "spill over" hypothesis, we look at attacks against *all other sectors*, excluding victims in the government, finance, media, energy, and utility sectors. We report the coefficients for the average number of daily attacks by Russia-based groups against victims in these sectors based on a full model specification (Figure 5).

These results show that there is a slight increase in the daily number of attacks by Russia-based groups against government targets in the two and one month periods before elections, although the effect size is relatively small (only about a 3% increase one month before an election). As for attacks intended to cause chaos and targeted against victims in the media, finance, energy, and utility sectors, there is no evidence that Russia-based groups increase attacks against these victims in the months before an election; in fact, there is actually a statistically significant *decrease* in the average number of daily attacks against these targets in the three months before an election. Lastly, we consider attacks against victims in all other sectors and find that there is a statistically significant *increase* in the average number of daily attacks by Russia-based groups, offering tentative support for the "spillover" hypothesis.

Thus, our empirical results suggest that the increase in attacks by Russia-based groups before elections may be partially explained by an increased focus on targeting election infrastructure, although it seems much of what is driving this pattern may be a spillover effect from the actions of Russian cybercriminals who also carry out other cyber exploits for the Russian government. We do not find evidence to support the hypothesis that an increase in attacks by Russia-based groups is part of an effort to create chaos or social unrest before elections.

6 Conti Leaks

To complement our quantitative analysis, we examine leaked chat logs from one of the most prolific ransomware groups, Conti. Conti first emerged as a descendent of a previous ransomware family, Ryuk, in July 2020 (Abrams 2022) and amassed an estimated $180 million dollars worth of cryptocurrency through its attacks (Burgess 2022b). In a little less than two years, Conti attacked over 1,000 victims, including Fortune 500 companies and the Irish Health Service Executive, which disrupted activity at hospitals across Ireland (Krebs 2022b). In light of Conti's sustained and destructive attacks, the U.S. government offered a reward of up to $15 million in May 2022 for information that could lead to arrests of Conti's members (Gatlan 2022).

Although the Russian-speaking cybercriminal community has long been closely aligned, Russia's invasion of Ukraine in late February 2022 brought tensions between Russians and Ukrainians into sharp relief, including in the criminal underworld (Waterman 2022). Soon after the invasion, Conti's leaders took the unusual step of declaring the group's allegiance to Russia through a message posted on its site on the dark web; this message also expressed the group's commitment to carrying out cyberattacks against any entity that attacked Russia. Although Conti's leaders later walked back this statement in favor of a more modest expression of support for Russia, the damage appears to have already been done in the eyes of at least one Ukrainian group member, who shared the group's chat logs, training manuals, and ransomware source code with a Ukrainian security researcher; soon after, the security researcher published these files online (Abrams 2022).

Office Politics

Conti's leaked chat logs contain over 60,000 messages and span communications between January 29, 2021 and February 27, 2022, providing unprecedented insight into the daily operations of a highly successful ransomware group (Abrams 2022; Burgess 2022b). Over the course of a year, the group's size fluctuated between 65 and 100 members, with each performing one of many differentiated roles (Krebs 2022c). At the bottom of the organization, coders built the group's online infrastructure, including encryption keys, dashboards, and other tools, while testers performed checks to ensure the group's tools were functioning as expected and remained undetectable by anti-virus software and other security tools (Krebs 2022b). Mid-level managers led operational teams within the organization, montioring progress by team members and reporting to upper management on big-picture topics. At the top of the organization, a boss called Stern (all group members went by pseudonyms) strategized future directions for the group – including developing a new cryptocurrency platform that would allow them to more easily launder funds (Krebs 2022d; Waterman 2022). Other roles in the organization included researchers – who were tasked with developing the aforementioned blockchain platform, penetration testers or "pentesters" – who worked in teams to steal data from companies targeted by the group, and recruiters – as the group was frequently in need of new employees (Krebs 2022b).

Conti's recruitment process was surprisingly professionalized. Recruiters often visited online job boards and reviewed resumes posted to these sites to identify potential recruits with desirable technical skills (Figueroa, Bing, and Silvestrini 2022). All potential recruits were then directed to participate in an online screening and interview process (conducted through encrypted chats to ensure anonymity), during which recruits were typically not informed of the group's illegal activity. If the applicant passed the interview, she was then hired and sent through a new hire training program complete with a training manual and onboarding by an employee working in a similar role (Figueroa, Bing, and Silvestrini 2022). Given the group's lack of forthrightness about the nature of its work, it is perhaps unsurprising that the group suffered from a high turnover rate (Krebs 2022b).

The chats also reveal information about the group's finances, including negotiations with victims and discussions about the lowest payment the group would be willing to accept in each case (Krebs 2022c); the following message shows an example of a discussion by group members about what to say to a victim:

> We are glad that you understand that your situation is not so sunny as it can be. Also, I think you understand that every day of negotiations will bring more and more losses, maybe even exponentially, so yes – you will gain a profit if you cooperate with us. However, 900,000 USD is not an satisfying offer too. We said

> our word - we are not interested in such a numbers. Try your best and raise it to a number with 7 zeroes minimum.

The chats also detail members' salaries, which were paid on the first and fifteenth of each month via cryptocurrency (Krebs 2022b). At one point, mid-level manager Mango reported payroll for his team to his boss, revealing that coders made between $1,000-$2,500 per month; elsewhere, it was revealed that Mango himself made roughly $54,000 per month (Waterman 2022). Based on the salary amounts for this team and the number of employees in the organization, estimates suggest that yearly operating costs for the group totaled roughly $6 million (Figueroa, Bing, and Silvestrini 2022). Given that the group took is believed to have received $180 million in 2021 (Krebs 2022b), this suggests that a large portion of the group's funds went to "upper level management."

Thus, in many ways, Conti appears to have functioned like a medium-sized software company (Waterman 2022). The organization maintained employees in a range of differentiated roles and made bimonthly payroll. In fact, much of the information contained in these chats is akin to mundane office chatter. Employees discussed price negotiations with "clients" (the tongue-in-cheek way that some groups refer to their victims) and affiliates (other ransomware groups); employees also requested time off and holiday bonuses and complained about long working hours. Managers, meanwhile, lamented that their employees were often unreachable and requested frequent updates from their team members (Krebs 2022b). However, amidst these banal discussions, evidence of the group's connections to the Russian government emerges.

Connections to the Russian Government

In one exchange, Mango discusses an FSB request to hack a Dutch journalistic organization, Bellingcat, with top Conti leader, Stern; the FSB was particularly interested in the organization's investigation into the poisoning of Russian opposition Alexei Navalny, which was carried out by the FSB. Mango and Stern agree to cooperate because they are "patriots" and later turn over stolen documents from the organization to the FSB (Burgess 2022b; Vedere Labs 2022). Sometime later, the group's leaders discuss receiving a payment from an external "partner," as well as the possibility that this unknown partner will likely provide more support to the group in the future (Burgess 2022a). Although unclear, this partner might be a division of the Russian government.

The chats reveal other connections between the Russian government and Conti leadership, as Stern received information from a government insider that Russian police had reopened a case against the group at the request of the United States (Vedere Labs 2022); importantly, Stern received confirmation from his source that the group would not be seriously investigated, but he was advised to "lay low" for at least ten days (Krebs 2022a). Conti's leaders were also informed of the actions of state-backed hackers like Cozy Bear (Burgess 2022a). Thus, Conti's leaders received valuable information and assurances from the Russian government.

Indeed, the evidence in this case matches a pattern of collaboration between the Kremlin and Russian cybercriminals and in other cases. Most notably, in 2017, the U.S. Department of Justice (DOJ) indicted four individuals for a 2014 hack against Yahoo that compromised 500 million user accounts, including sensitive information about journalists and government officials in the United States and Russia (Bajak 2021). The indictment reveals that two FSB officers recruited a Russian national, Alexseyvich Belan, to carry out the hack; Belan had previously been indicted by the DOJ for cybercrimes in 2012 and arrested by a European country in 2013, but he had managed to flee to Russia before facing extradition. In Russia, the authorities not only refused to arrest Belan as the U.S. and Interpol had requested, but instead, they recruited him to participate in their own hack (Department of Justice 2017). In exchange for his cooperation, the FSB shared information with Belan about the U.S. case against him and allowed Belan to enrich himself though the hack. The fourth person, a Canadian national, was paid by the FSB for his participation in the hack (Maurer 2018).

While the Yahoo hack reveals the depth of ties between the FSB and Russian criminals in one particular case, connections between the FSB and cybercriminals have long been rumored. Experts note that the Kremlin sometimes enlist cybercriminals by giving them a choice between prison and working for the Russian government, and government employees have been known to "moonlight" as cybceriminals to earn extra income on the side (Bajak 2021). Thus, the Russian government more generally and the FSB in particular have maintained nebulous connections to Russian-speaking cybercriminals.

However, the Russian government's relationship with Russia-based ransomware groups also differs in important ways from its relationship with state-backed cyber actors, which it has employed on multiple occasions. For example, two Russian government agencies – Russia's military intelligence agency (the GRU) and Russia's Foreign Intelligence Service (the SVR) – maintain cyber groups (known as Fancy Bear and Cozy Bear respectively) that carry out politically-motivated cyber attacks for the Russian government (CrowdStrike n.d.; CrowdStrike Editorial Team 2019).

Unlike these actors, however, ransomware groups are not directly linked to a Russian government agency and do not take orders directly from the government. Instead, ransomware groups operate as independent criminal groups but will occasionally perform favors for the Kremlin in exchange for broad guarantees, such as protection from domestic and international prosecution. The Russian government, meanwhile, obtains plausible deniability from some of its most controversial foreign objectives – namely meddling that challenges other states' sovereignty. Thus, we argue that the relationship between the Russian government and Russia-based ransomware groups most closely resemble a set of *loose ties* connecting both parties in a mutually beneficial relationship.

7 Conclusion

In short, this paper probes for connections between the political motivations of the Russian state and the targeting choices of ransomware groups based in Russia. We find evidence suggestive of loose ties between the Russian government and Russia-based groups – namely an increase in the number of attacks by Russia-based groups before elections across six major democracies. Further, the analysis of leaked chat logs from one of the biggest Russia-based ransomware groups suggests an informal relationship between the two. Through this research, we hope to advance a broader understanding of the nature of international cyber security threats faced today.

References

Abrams, Lawrence (2022). "Conti ransomware's internal chats leaked after siding with Russia". In: URL: https://www.bleepingcomputer.com/news/security/conti-ransomwares-internal-chats-leaked-after-siding-with-russia/.

Ashraf, Cameran (2021). "Defining cyberwar: towards a definitional framework". In: *Defense & Security Analysis* 37.3, pp. 274–294.

Auchard, Eric (2017). "Macron campaign was target of cyber attacks by spy-linked group". In: *Reuters World News*.

Bajak, Frank (2021). "How the Kremlin provides a safe harbor for ransomware". In: *AP News*. URL: https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999.

Ballard, Mark (2019). "No data lost, no ransom paid in Louisiana cyber attack; Ardoin says no impact on state elections". In: *The Advocate*. URL: https://www.theadvocate.com/baton_rouge/news/politics/legislature/article_9c29ac24-0d6b-11ea-ad3c-47019c29d7ef.html.

Barnes, Julian E (2020). "Russia is trying to steal virus vaccine data, Western nations say". In: *The New York Times* 16.2020, pp. 11–10.

Bing, Christopher (2019). "Exclusive: US Officials Fear Ransomware Attack Against 2020 Election". In: *Reuters*. URL: https://www.reuters.com/article/us-usa-cyber-election-exclusive/exclusive-u-s-officials-fear-ransomware-attack-against-2020-election-idUSKCN1VG222.

Bing, Christopher and Raphael Satter (2019). "Louisiana government computers knocked out after ransomware attack". In: *Reuters*. URL: https://www.reuters.com/article/us-usa-louisiana-cyberattack/louisiana-government-computers-knocked-out-after-ransomware-attack-idUSKBN1XS2LA.

Borghard, Erica D and Shawn W Lonergan (2017). "The logic of coercion in cyberspace". In: *Security Studies* 26.3, pp. 452–481.

— (2021). "Deterrence by denial in cyberspace". In: *Journal of Strategic Studies*, pp. 1–36.

Brunton, Finn (2013). "The long, weird history of the Nigerian e-mail scam". In: URL: https://www.bostonglobe.com/ideas/2013/05/18/the-long-weird-history-nigerian-mail-scam/C8bIhwQSVoygYtrlxsJTlJ/story.html.

Bumiller, Elisabeth and Thom Shanker (2012). "Panetta Warns of Dire Threat of Cyberattack on U.S." In: *The New York Times*. URL: https://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

Burgess, Matt (2022a). "Leaked Ransomware Docs Show Conti Helping Putin From the Shadows". In: URL: https://www.wired.com/story/conti-ransomware-russia/.

— (2022b). "The Big, Baffling Crypto Dreams of a $180 Million Ransomware Gang". In: URL: https://www.wired.com/story/conti-ransomware-crypto-payments/.

Caesar, Ed (2021). "The Incredible Rise of North Korea's Hacking Army". In: *The New Yorker*. URL: https://www.newyorker.com/magazine/2021/04/26/the-incredible-rise-of-north-koreas-hacking-army.

Clark, David D and Susan Landau (2011). "Untangling attribution". In: *Harv. Nat'l Sec. J.* 2, p. 323.

Clayton, Mark (2014). "Ukraine election narrowly avoided 'wanton destruction' from hackers". In: *The Christian Science Monitor*. URL: https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

Cornish, Paul et al. (2010). *On cyber warfare*. Chatham House London.

CrowdStrike (n.d.). *Adversary: Cozy Bear*. URL: https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/.

CrowdStrike Editorial Team (2019). *Who is FANCY BEAR (APT28)?* URL: https://www.crowdstrike.com/blog/who-is-fancy-bear/.

Department of Justice (2017). *U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts.* URL: https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

— (2018). "Nine Iranians Charged With Conducting Massive Cyber Theft Campaign On Behalf Of The Islamic Revolutionary Guard Corps". In: URL: https://www.justice.gov/usao-sdny/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic.

Dixon, Robyn and Ellen Nakashima (2022). "Russia arrests 14 alleged members of REvil ransomware gang, including hacker U.S. says conducted Colonial Pipeline attack". In: URL: https://www.washingtonpost.com/world/2022/01/14/russia-hacker-revil/.

DOJ Office of Public Affairs (2021). *Ukrainian Arrested and Charged with Ransomware Attack on Kaseya.* URL: https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

Egloff, Florian J and Max Smeets (2021). "Publicly attributing cyber attacks: a framework". In: *Journal of Strategic Studies*, pp. 1–32.

Elswah, Mona and Philip N Howard (2020). ""Anything that causes chaos": The organizational behavior of Russia Today (RT)". In: *Journal of Communication* 70.5, pp. 623–645.

Federal Bureau of Investigation (2022). "Internet Crime Report 2021". In: URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

Figueroa, Marco, Napoleon Bing, and Bernard Silvestrini (2022). *The Conti Leaks: Insight into a Ransomware Unicorn.* URL: https://www.breachquest.com/blog/conti-leaks-insight-into-a-ransomware-unicorn/.

Fung, Brian (2020). "Ransomware hits election infrastructure in Georgia county". In: *CNN Business.* URL: https://www.cnn.com/2020/10/22/tech/ransomware-election-georgia/index.html.

Gartzke, Erik (2013). "The myth of cyberwar: bringing war in cyberspace back down to earth". In: *International security* 38.2, pp. 41–73.

Gartzke, Erik, Jon Lindsay, and Michael Nacht (2014). "Cross-Domain Deterrence: Strategy in an Era of Complexity". In: *International Studies Association Annual Meeting, Toronto.*

Gartzke, Erik and Jon R Lindsay (2015). "Weaving tangled webs: offense, defense, and deception in cyberspace". In: *Security Studies* 24.2, pp. 316–348.

Gatlan, Sergui (2022). "US offers $15 million reward for info on Conti ransomware gang". In: URL: `https://www.bleepingcomputer.com/news/security/us-offers-15-million-reward-for-info-on-conti-ransomware-gang/`.

Gorwa, Robert and Max Smeets (2019). "Cyber conflict in political science: a review of methods and literature". In.

INTERPOL (2021). *Joint global ransomware operation sees arrests and criminal network dismantled.* URL: `https://www.interpol.int/en/News-and-Events/News/2021/Joint-global-ransomware-operation-sees-arrests-and-criminal-network-dismantled`.

Krebs, Brian (2021). *Try This One Weird Trick Russian Hackers Hate.* URL: `https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/`.

— (2022a). *Conti Ransomware Group Diaries, Part I: Evasion.* URL: `https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/`.

— (2022b). *Conti Ransomware Group Diaries, Part II: The Office.* URL: `https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-ii-the-office/`.

— (2022c). *Conti Ransomware Group Diaries, Part III: Weaponry.* URL: `https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iii-weaponry/`.

— (2022d). *Conti Ransomware Group Diaries, Part IV: Cryptocrime.* URL: `https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-iv-cryptocrime/`.

Krebs, Brian (2022e). *Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison.* URL: `https://krebsonsecurity.com/2022/03/estonian-tied-to-13-ransomware-attacks-gets-66-months-in-prison/`.

Lakshmanan, Ravie (2021). "Ukraine Police Arrest Cyber Criminals Behind Clop Ransomware Attacks". In: URL: `https://thehackernews.com/2021/06/ukraine-police-arrest-cyber-criminals.html`.

— (2022). "Husband-Wife Arrested in Ukraine for Ransomware Attacks on Foreign Companies". In: URL: `https://thehackernews.com/2022/01/husband-wife-arrested-in-ukraine-for.html`.

Libicki, Martin C (2009). *Cyberdeterrence and cyberwar.* RAND corporation.

Lindsay, Jon R (2013). "Stuxnet and the limits of cyber warfare". In: *Security Studies* 22.3, pp. 365–404.

Lindsay, Jon R and Erik Gartzke (2016). "Coercion through cyberspace: The stability-instability paradox revisited". In: *The Power to Hurt: Coercion in Theory and in Practice*, pp. 176–204.

— (2020). "Politics by many other means: The comparative strategic advantages of operational domains". In: *Journal of Strategic Studies*, pp. 1–34.

Lonergan, Erica D and Shawn W Lonergan (2022). "Cyber Operations, Accommodative Signaling, and the De-Escalation of International Crises". In: *Security Studies* 31.1, pp. 32–64.

Marks, Joseph (2019). "The Cybersecurity 202: Ransomware attack against the 2020 election could disrupt statewide voting databases". In: URL: `https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/09/06/the-cybersecurity-202-ransomware-attack-against-the-2020-election-could-disrupt-statewide-voting-databases/5d713c4d602ff171a5d7343d/`.

Maurer, Tim (2018). “Why the Russian government turns a blind eye to cybercriminals”. In: *Slate,(February 2, 2018), retrieved from https://slate. com/technology/2018/02/why-the-russian-government-turns-a-blind-eye-to-cybercriminals. html.*

McGuinness, Damien (2017). “How a cyber attack transformed Estonia”. In: *BBC News.* URL: `https://www.bbc.com/news/39655415`.

McMillan, Robert and Dustin Volz (2022). “Google Sees Russia Coordinating With Hackers in Cyberattacks Tied to Ukraine War”. In: URL: `https://www.wsj.com/articles/google-sees-russia-coordinating-with-hackers-in-cyberattacks-tied-to-ukraine-war-11663930801`.

Mehrotra, Kartikay (2020). “Hacks on Louisiana Parishes Hint at Nightmare Election Scenario”. In: *Bloomberg.* URL: `https://www.bloomberg.com/news/articles/2020-02-11/hacks-on-louisiana-parishes-hint-at-nightmare-election-scenario#xj4y7vzkg`.

Miller, Maggie (2021). “International coalition arrests hackers linked to thousands of ransomware attacks”. In: URL: `https://thehill.com/policy/cybersecurity/580545-international-coalition-arrests-hackers-linked-to-thousands-of/`.

Mueller, Robert S et al. (2019). *The Mueller Report.* e-artnow.

Nechepurenko, Ivan (2022). “Russia Says It Shut Down Notorious Hacker Group at U.S. Request”. In: *The New York Times.* URL: `https://www.nytimes.com/2022/01/14/world/europe/revil-ransomware-russia-arrests.html`.

Perlroth, Nicole and David E. Sanger (2020). “Ransomware Attacks Take On New Urgency Ahead of Vote”. In: *The New York Times.* URL: `https://www.nytimes.com/2020/09/27/technology/2020-election-security-threats.html`.

Rid, Thomas (2012). “Cyber war will not take place”. In: *Journal of strategic studies* 35.1, pp. 5–32.

Rid, Thomas and Ben Buchanan (2015). “Attributing cyber attacks”. In: *Journal of Strategic Studies* 38.1-2, pp. 4–37.

Robinson, Tom (2021). “How Iran Uses Bitcoin Mining to Evade Sanctions and “Export” Millions of Barrels of Oil”. In: URL: https://www.elliptic.co/blog/how-iran-uses-bitcoin-mining-to-evade-sanctions.

Rogin, Josh (2012). “NSA Chief: Cybercrime constitutes the “greatest transfer of wealth in history””. In: *Foreign Policy.* URL: https://foreignpolicy.com/2012/07/09/nsa-chief-cybercrime-constitutes-the-greatest-transfer-of-wealth-in-history/.

Rosenberg, Matthew, Nicole Perlroth, and David E Sanger (2020). “‘Chaos is the Point’: Russian hackers and trolls grow stealthier in 2020”. In: *The New York Times.* URL: https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

Sanger, David E. and Nicole Perlroth (2020). “Microsoft Takes Down a Risk to the Election, and Finds the U.S. Doing the Same”. In: *The New York Times.* URL: https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html.

Schectman, Joel and Christopher Bing (2022). “EXCLUSIVE Ukraine calls on hacker underground to defend against Russia”. In: *Reuters.* URL: https://www.reuters.com/world/exclusive-ukraine-calls-hacker-underground-defend-against-russia-2022-02-24/.

Select Committee on Intelligence United States Senate (2020). “Russian Active Measures Campaigns and Interference in the 2016 U.S. Election, Volume 2: Russia’s Use of Social Media with Additional Views”. In: URL: https://www.intelligence.senate.gov/sites/default/files/documents/Report_Volume2.pdf.

Selesky, Andrew (2022). “Hackers hit web hosting provider linked to Oregon elections”. In: *AP News.* URL: https://apnews.com/article/2022-midterm-elections-technology-oregon-primary-campaign-finance-2569fb52de35e066928a8ffcc5c1febb.

Solis, Gary D (2014). “Cyber warfare”. In: *Mil. L. Rev.* 219, p. 1.

Stahl, Jeremy (2020). "The 10 Scariest Election Scenarios, Ranked". In: *SLATE*. URL: https://slate.com/news-and-politics/2020/08/election-nightmares-experts.html.

Stone, John (2013). "Cyber war will take place!" In: *Journal of strategic studies* 36.1, pp. 101–108.

Toulas, Bill (2021). "Police arrest hackers behind over 1,800 ransomware attacks". In: URL: https://www.bleepingcomputer.com/news/security/police-arrest-hackers-behind-over-1-800-ransomware-attacks/.

Tsagourias, Nicholas (2012). "Cyber attacks, self-defence and the problem of attribution". In: *Journal of conflict and security law* 17.2, pp. 229–244.

Vedere Labs (2022). *Analysis of Conti Leaks*. URL: https://www.forescout.com/resources/analysis-of-conti-leaks/.

Waterman, Shaun (2022). *Inside the Conti leaks rattling the cybercrime underground*. URL: https://readme.security/the-conti-leaks-first-rumble-of-the-ukraine-earthquake-thats-rattling-the-cybercrime-underground-7abb23b0fb04.

White, Geoff and Jean H. Lee (2021). "The Lazarus heist: How North Korea almost pulled off a billion-dollar hack". In: *BBC News*. URL: https://www.bbc.com/news/stories-57520169.

Wray, Christopher (2020). "The Threat Posed by the Chinese Government and the Chinese Communist Party to the Economic and National Security of the United States". In: URL: https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states.

Zetter, Kim (2015). "Hackers Finally Post Stolen Ashley Madison Data". In: URL: https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/.

A Victims by Country

Table 12: Victim Count by Country

Rank	Country	Count	Percent
1	USA	2,048	51.3
2	Canada	231	5.8
3	Great Britain	200	5.0
4	France	192	4.8
5	Germany	183	4.6
6	Italy	165	4.1
7	Austria	78	2.0
8	Spain	74	1.9
9	Brazil	62	1.6
10	Indonesia	49	1.2
	All other countries	707	18.2

B Victims by Sector

Table 13: Victim Count by Sector

Sector	Count	Percent	Industry Group
Industrials	1,084	27.0	Capital goods, commercial and professional services, transportation
Consumer Discretionary	621	15.5	Automobiles and components, consumer durables and apparel, consumer services, retailing
Other Services	362	9.0	Other professional services, charities and non-profits, religious and native groups or organizations, other social or development organizations
Materials	305	7.6	Materials
Information Technology	292	7.3	Software and services, technology hardware and equipment, semiconductors and semiconductor equipment
Health care	252	6.3	Health care equipment and services; pharmaceuticals, biotechnology and life sciences
Financials	229	5.7	Banks, diversified financials, insurance
Consumer Staples	196	4.9	Food and staples retailing; food, beverage and tobacco; household and personal products
Public Administration	163	4.1	Law enforcement and first responders; government administration; other public administration
Education	150	3.7	Primary and secondary education; tertiary (post-secondary) education; education services
Communication Services	114	2.8	Telecommunication services; media and entertainment
Real Estate	101	2.5	Real estate
Energy	79	2.0	Energy
Utilities	71	1.8	Utilities