Assessing the Political Motivations Behind Ransomware Attacks*

Karen Nershi† & Shelby Grossman‡

July 13, 2023

Abstract

Although traditionally viewed as apolitical, recent developments suggest there may be connections between some ransomware groups and the Russian government. To better understand this relationship, we created a dataset of 4,194 ransomware victims posted to the dark web between May 2019 and May 2022. We find that Russia-based ransomware groups increased attacks before elections in several major democracies, and companies that curtailed operations in Russia after the invasion of Ukraine were more likely to be targeted; these findings suggest potential political motivations behind these attacks. We also analyze a major ransomware group's leaked internal communications, which show ties to the Kremlin. We argue that the Russian government maintains an informal cooperative relationship with groups by providing safe harbor from prosecution and receiving plausible deniability for attacks and access to skilled cyber actors. Our findings suggest ransomware presents an international security threat in addition to functioning as a form of crime.

*We are grateful to Allan Liska, Charles Littrell, David Skarbek, Erik Gartzke, Hadi Elzayn, Jacob N. Shapiro, Jelena Vićić, John Guyton, John Hultquist, John Perrino, Jon R. Lindsay, Justin Key Canfil, Matthew Collin, Renee DiResta, Robert Hayden, and Sanne Verschuren for comments on this draft. For data collection and research assistance, we thank David Thiel, Caroline Meinhardt, Miles McCain, and Michaela Robinson. We thank Chainalysis for providing access to data.

†Stanford University and IE University. karen.nershi@ie.edu

‡Stanford University. shelbygrossman@stanford.edu

1 Introduction

Hours after polls closed in Louisiana's 2019 gubernatorial election, a ransomware attack brought down 10% of the state's computer servers and prompted the governor to declare a state of emergency (Ballard 2019; Bing and Satter 2019). This attack followed a seemingly unrelated one, in which a breach of a Louisiana state contractor allowed attackers to access servers across the state; although the attackers had gained access to these servers months earlier, they waited until six days before the election to launch a ransomware attack (Mehrotra 2020). Although neither attack prevented the state from tallying votes or certifying results, they highlight that ransomware, which is often considered an apolitical crime, may also have political motivations.

Ransomware is a type of malware that encrypts a user's files; attackers then demand to be paid a ransom (typically in cryptocurrency) before sharing the decryption key with a victim. While many early ransomware attacks targeted individuals, attacks in recent years have primarily targeted companies, including multi-billion dollar companies (Loui and Reynolds 2021). A clear geopolitical dimension of these attacks has also emerged, with many attacks originating in Eastern Europe and targeting companies in Western countries. While there are several reasons for the prevalence of cybercriminals in Eastern Europe – including a supply of highly skilled graduates from technical universities founded during the Soviet era, a lack of technical jobs in the private sector, and weak law enforcement (Kostyuk and Geers 2015) – Russia stands out in the region due to its refusal to cooperate with Western countries to arrest criminals behind ransomware attacks, who typically work together in groups. Although Western countries have never directly implicated the the Russian government in these attacks, the Russian government's relationship with ransomware groups remains ambiguous and has attracted international scrutiny.

In this paper, we ask: what is the relationship between the Russian government and Russia-based ransomware groups? Relatedly, what aspects of ransomware attacks (if any)

cannot be explained by financial motives alone? Our research contributes to scholarship on the relationship between states and criminal groups. Specifically, we argue that states' cooperation with cybercriminal groups does not undermine the strength of state institutions in the same way as cooperation with traditional criminal groups because cybercriminal groups conduct most of their activities online rather than within the state's physical territory. By cooperating with cybercriminal groups, states can benefit from plausible deniability for government cyber operations that involve ransomware groups and groups' ability to specialize in relevant skills that would be more difficult to obtain through in-house operations.

To better understand the relationship between the Kremlin and ransomware groups, we created a new dataset of the victims of ransomware attacks. One of the major challenges for researchers has been a lack of reliable data about cyber attacks, as prior datasets have relied on public reporting or disclosures by victims themselves. However, victims are often reluctant to report attacks given the risk of reputational harm or legal liability. To avoid this bias, we collected information about the victims of a specific type of ransomware attack known as a "double extortion" attack. In a double extortion attack, ransomware groups post about their victims on the dark web as part of the extortion process. We leveraged these sites to create a dataset of all victims of double extortion attacks posted to these sites between November 2021 and April 2022, and we merge this dataset with another from cybersecurity firm Dark Tracer. Our dataset improves on prior research by offering complete coverage for one particular type of cyber attack during the data collection period.

Using this dataset, we perform statistical tests to detect trends in the targeting of these attacks that are unlikely to be explained by financial motivations alone. First, we find an increase in the number of attacks by Russia-based ransomware groups before elections in several major democracies, with no similar increase in attacks by other groups. This suggests that Russia-based ransomware groups may increase attacks before elections as part of state-backed efforts aimed at election meddling. Second, we find a decrease in the number of daily ransomware attacks after Russia's invasion of Ukraine, which we argue is likely driven

by Russia's recruitment of ransomware operators to aid its cyber offensive against Ukraine. Third, we find that companies that withdrew from or suspended operations in Russia after the invasion were more likely to experience a ransomware attack in the months after the invasion; this suggests that ransomware groups may have retaliated against these companies (as these actions were widely perceived as a condemnation of the invasion).

We also analyze a trove of of over 60,000 leaked messages from a prolific Russia-based ransomware group, Conti. The internal communications, which were sent between 2020 and 2022, provide insight into the group's structure and operations, including connections to the Kremlin. Multiple Conti leaders communicated with Russian government contacts and discussed cooperation on several state-backed cyber operations, although Conti was an independent criminal organizations that focused primarily on extorting victims for profit. In addition to providing insight into the group's relationship with the Russian government, our analysis contributes to scholarship on the inner workings of criminal and other violent groups using primary source documents (Lessing and Willis 2019; Levitt and Venkatesh 2000; Johnston et al. 2016; Al-Tamimi 2015). Further, the quotidian dialog of the chat logs provide insight into the thoughts and actions of group leaders and low-level members in a way generally not possible from previous document troves that have detailed criminal groups' record keeping (Lessing and Willis 2019; Levitt and Venkatesh 2000).

Based on our analyses, we argue that the Kremlin maintains decentralized yet cooperative relations with ransomware groups. We theorize that the chief benefit the Russian government provides to ransomware groups is safe harbor from domestic and foreign prosecution, a benefit that has increased in value as Western law enforcement has increasingly targeted cybercriminals. In return, the Kremlin benefits from plausible deniability for state-backed cyber operations as well as access to specialized skills, from which it can recruit operators to carry out cyber missions. Further, the Kremlin benefits indirectly from the fact that groups primarily target victims in Western countries. Russia's tacit cooperation with ransomware groups means that ransomware is not only a form of crime – it is also an international

security risk as states play a role in how some crimes are committed.

The rest of the paper is structured as follows. In Section 2, we survey the literature on relations between political actors and criminal groups and present a theory of how and why states may ally with cybercriminal groups. In Section 3, we discuss our new dataset, and in Section 4, we present our analysis. In Section 5, we provide insights from internal communications leaked from a major ransomware group. In Section 6, we discuss the our findings and provide concluding thoughts.

2 Criminal Groups and the State

Drawing on the European experience, Charles Tilly (1985) theorizes that state-building was an iterative process through which national governments centralized power by eliminating internal rivals, allowing national governments to gain a monopoly over the use of violence. Although the theory has become widely influential, a key premise of Tilly's argument – that states eliminate criminal groups as part of the state-building process – has little relevance to the experience of many, especially in Latin America. Indeed, research shows that not only do criminal groups exist in modern states, they can exercise significant influence over both politics and public life.[1] Accordingly, research in recent years has explored the role of criminal groups in modern states, with one strain focusing on the types of relationships that develop between criminal groups and political actors. These relationships have been wide-ranging – with criminals alternately bribing or coercing politicians, colluding with political parties, and waging war against national governments – and these relationships, in turn, have shaped levels of violence and political outcomes (Barnes 2017).

We build on this research by expanding analysis into a new area: that of a state's relationship with *cyber*criminal groups. Specifically, we ask: why might a state choose

[1]For example, see Dal Bó, Dal Bó, and Di Tella (2006), Dube, Dube, and García-Ponce (2013), Ley (2018), Trejo and Ley (2018), and Trejo and Ley (2021). For examples of research examining the role of criminal groups in other contexts, see Gambetta (1993), Varese (2018), and Skarbek (2011).

to cooperate with a cybercriminal group, and what are the risks? Through our analysis, we show that a state's relationship with a cybercriminal group minimizes a risk inherent to cooperation with traditional criminal groups: harm to state institutions. States can also access a different set of "services" than those provided by traditional criminal groups. Lastly, states can benefit from plausible deniability and access to a pool of specialized talent through cooperation with cybercriminal groups.

2.1 Benefits and Risks of Cooperation with Criminal Groups

Why might a state choose to cooperate with a criminal group? While individual politicians may be coerced by violence or threats of violence, collaboration with criminal groups at higher levels of government is typically based on an exchange of favors. Specifically, political actors provide access and other selective benefits to criminal groups, while groups provide illegal (often violent) services for their political allies. Although there are few cases of outright collaboration between states and criminal groups,[2] research shows collaboration between political parties and criminal groups across a range of contexts.[3] In these contexts, the services provided by criminal groups are typically aimed at helping political parties win elections, including through vote buying and the violent intimidation of other candidates, parties, and even the voting public.

Political parties have also turned to criminal groups for other types of violent services. In post-war Japan, conservative parties engaged members of the yakuza to intimidate members of rival political parties and disrupt protests that threatened their political agenda (Siniawer

[2]Varese (2018) identifies Somalia and Burma as examples of "mafia states," in which criminals have become integrated within the state apparatus, and the state itself participates in crime.

[3]Examples of such relationships include the cartels and the Institutional Revolutionary Party (PRI) in Mexico (Trejo and Ley 2018; Ley 2018), the mafia and the Christian Democratic Party in Italy (De Feo and De Luca 2017; Dipoppa 2021), the yakuza and conservative parties in Japan (Siniawer 2012), as well as multiple criminal groups and political parties across Colombia (Nieto-Matiz 2022) and Brazil (Albarracín 2018).

2012). Meanwhile, in post-war Italy, the Christian Democratic Party leveraged connections with mafia groups to disrupt labor strikes and supply informal labor, undermining the power of organized labor (Dipoppa 2021). Similarly, political parties in Russia have commissioned the Russian mafia to disrupt labor strikes and intimidate members of other parties, especially the labor party (Varese 2018, p. 172).

However, by cooperating with criminal groups, states run the risk of weakening state institutions. Indeed, the benefits that political actors provide to criminal groups – including selective enforcement of the law and access to state resources (e.g., public contracts) – often weaken the state through degradation of the rule of law. Meanwhile, criminal groups that extort local businesses deplete the state's tax base, and groups that provide governance to subnational populations like residents of poor neighborhoods challenge the state's authority and legitimacy in the eyes of populations under their control.[4] Thus, criminal groups present a competing source of power within states (Tilly 1985), and states that cooperate with them risk depleting their capacity.

2.2 A Theory of Cooperation with Cybercriminal Groups

We argue that a state's relationship with cybercriminal groups differs from relationships with traditional criminal groups in two key ways. First, unlike with traditional criminal groups, a state's cooperation with a cybercriminal group does not directly threaten the strength of state institutions because cybercriminals operate in cyberspace, which is an extraterritorial space. Indeed, in the 1990s, international law scholars often used "space" or "place" metaphors to describe cyberspace, highlighting the unique legal and operational challenges that states face when attempting to regulate online activity (Cohen 2007). And although government control of online spaces has greatly increased over the last two decades, vast swaths of the internet remain unregulated; thus, cybercriminals operating online do not directly challenge

[4]For research on subnational governance by criminal groups, see Skarbek (2011), Lessing (2021), Skarbek (2016), Magaloni, Franco-Vivanco, and Melo (2020), Lessing (2015), and Arias (2006).

the power of state institutions in the same way that traditional criminal groups operating within a state's territory do.

Second, a state's relationship with cybercriminal groups differs from those with traditional criminal groups in that cybercriminals groups provide *non-violent* illegal services primarily aimed at *foreign actors* rather than domestic ones. Traditional criminal groups typically rely on violence to influence local populations in ways that benefit their political allies. Cybercriminal groups, by contrast, offer non-violent hacking services that can be directed against foreign actors.

Drawing from the literature on influence operations and proxy conflict, we argue that states can achieve two key benefits through cooperation with cybercriminal groups. First, states can benefit from plausible deniability by engaging nonstate actors to carry out politically sensitive missions. We see this dynamic at play in Russia's relationship with the Internet Research Agency, a private company that it engaged to wage a propaganda campaign on social media during the U.S. 2016 presidential election; in the months and years that followed, Russia adamantly denied any involvement in election meddling (Mueller and Cat 2019; DiResta, Grossman, and Siegel 2022, p. 4). Russia has also deployed the Wagner Group, a private military contractor, to neighboring countries and international conflicts while denying any connection to the group (Marten 2019). The Wagner Group has committed human rights violations in Syria, but because the group is a private military corporation rather than a part of the Russian military, Russia avoided some international culpability (Hussain 2023).

Second, states can benefit from cooperation with cybercriminal groups by drawing on groups' ability to specialize. Because governments pursue a wide range of objectives, it is often too time consuming and costly for agents to specialize in skills for specific operations. However, by collaborating with nonstate actors, states can benefit from these actors' ability to specialize in relevant skills for specific operations. We see this in the context of Russia's relationship with the Internet Research Agency, as the organization leveraged cutting-edge

social media techniques to attract a larger audience for its content than content on similar themes generated by a division of the Russian military (DiResta, Grossman, and Siegel 2022). The Russian government has also benefited from Wagner's willingness to violate the rules of war (Marten 2019).

We examine this theory in the context of Russia's relationship with ransomware groups. And while other states *could* engage in similar relationships with ransomware groups, we expect that Russia is unique in this regard because of its willingness to outsource operations to nonstate actors and use unconventional tactics against its rivals. Notably, other countries willing to carry out cyber attacks (including China and North Korea) have adopted more tightly controlled policies toward cyber actors by employing them to work closely with government agencies to pursue state-sanctioned missions.[5] Thus, Russia's relationship with ransomware groups remains an outlier.

2.3 Hypotheses

To assess the possibility that groups originating in Russia have links to the Russian government, we measure the frequency of ransomware attacks before elections in several major democracies. There are several potential reasons why Russia-based groups may increase attacks before elections, including a state-backed effort to harm election infrastructure. Indeed, ransomware groups have targeted election contractors and election infrastructure before or during elections in several U.S. states, including Oregon (Selesky 2022), Louisiana (Bing and Satter 2019), Georgia (Fung 2020), and Florida (Perlroth and Sanger 2022). Attacks against election infrastructure or related targets could also create a *perception hack*, in which news of a cyber intrusion leads the public to question the reliability of election results regardless of the attack's actual impact. The Kremlin attempted such an attack during Ukraine's

[5]See for example Caesar (2021), U.S. Department of Justice (2021), U.S. Department of Justice (2020), Human Rights Watch (2022), Nakashima and Starks (2022), Marks (2022), Burges (2023), and Rising (2023).

2014 presidential election, when a hacked computer system nearly led the media to incorrectly report the election's winner on national television (Perlroth and Sanger 2022). Thus, Russia-based groups could increase attacks before elections in an effort to harm election infrastructure.

Another hypothesis for increased attacks before elections is that they result from a state-backed effort to create chaos in democracies during a politically sensitive time. Indeed, Russia has used cyber attacks to create disruptions across civil society during politically sensitive times in other countries, including Estonia and Georgia (Ottis 2008; Shakarian 2011; Markoff 2008). Increased attacks could also be driven by a spillover effect from other types of state-backed cyber activities before elections. Russian state-backed hackers have carried out other cyber attacks before elections, including a hack of the Democratic National Committee before the 2016 U.S. presidential election and a hack of Emanuel Macron's campaign before the 2017 French presidential election (Cerulus 2020; Nakashima and Harris 2018). Given connections between Russian state-backed cyber actors and cybercriminals,[6] exploits (which allow criminals to gain access to a computer system) from other state-backed cyber attacks could be re-purposed for apolitical ransomware attacks. Because exploits are typically time-sensitive and may be country specific, this could lead to a spike in ransomware attacks before elections. For any of these reasons, Russia-based groups may increase the number of ransomware attacks before elections in democratic countries.

On the other hand, ransomware groups may increase attacks before elections because they find it easier to extort victims before elections. For example, a media company might be more willing to pay a ransom if they sought to quickly restore news coverage of an election. If this explanation is true and attacks are driven primarily by profit, both Russia-based and other groups will likely increase attacks before elections in democratic countries.

To further probe potential political targeting in ransomware attacks, we test whether

[6]See U.S. Department of Justice (2017) for an example of a case involving connections between individuals working for the Russian government and cybercriminals.

companies that withdrew or suspended operations in Russia after the invasion were more likely to be targeted with ransomware. After the invasion, some companies chose to withdraw or suspend operations in Russia, and these actions were widely perceived as a condemnation of the invasion. If these companies were more likely to be targeted with ransomware after the invasion, this would suggest that groups may have retaliated against companies that took a stance perceived as critical of Russia.

3 Data

Most datasets of cyber attacks rely on media reports or disclosures made by victims themselves;[7] however, many victims are reluctant to disclose a cyber attack because they fear potential reputational harm or legal liability. Thus, these datasets are biased toward large attacks (that are more likely to receive media coverage). To address this challenge, we collected a dataset of cyber attacks using information from the ransomware groups, who reveal information about their victims as part of the extortion process.

Our dataset includes information about the victims of "double extortion" ransomware attacks, in which attackers exfiltrate data from a victim (typically a business or other organization) in addition to deploying encryption malware; attackers then threaten to post a victim's data online should the victim refuse to pay an additional (or more exorbitant) ransom.[8] As part of these attacks, groups post about their victims on sites on the dark web. Crucially, groups post information about victims currently under attack (not just those that fail to pay) – including a victim's name, website, and address – and typically only post a victim's stolen data if they fail to pay. To ensure the privacy of victims, we did not access stolen files and do not identify victims by name in our analysis.

[7] See for example Council on Foreign Relations (2021), Akoto (2022), and Valeriano, Jensen, and Maness (2018).

[8] All victims in the dataset are businesses or organizations rather than individuals because businesses are the primary targets of these attacks.

Figure 1: Ransomware Group Leak Sites

(a) Conti (b) Grief

Notes: Images show the "leak sites" of two ransomware groups, Conti and Grief, on the dark web. Groups post about their victims on these sites as part of the extortion process and threaten to release stolen data. Victims' names, addresses, and other identifying information have been withheld to protect their privacy.

We collected the data by visiting all known ransomware "leak sites" on the dark web daily between November 1, 2021 and April 30, 2022; collecting the data from each group's site ensures we also know each ransomware group's identity. Accordingly, our dataset contains the complete universe of double extortion victims posted to the dark web during the six month period. We then merged our dataset with an existing one collected in a similar way by cybersecurity firm Dark Tracer, which includes attacks between May 1, 2019 and July 23, 2021 (Dark Tracer Intelligence 2021). We obtained 421 victim matches across the two datasets, with 2,254 unique victims in the Dark Tracer dataset and 1,519 unique victims in our dataset for a total of 4,194 victims attacked between May 1, 2019 and April 30, 2022.

Although our dataset relies on information from criminal actors (who are not always truthful), we believe the data is reliable for several reasons. First, some of these attacks have been confirmed by other sources, including victims themselves. Second, some groups post "samples" of the files they exfiltrated from victims to these sites as proof of their attacks. Groups also typically post larger batches of files for victims they claim refused to

pay. Lastly, internal discussions from a ransomware group known as Conti confirm details about the extortion process of a typical group, which includes posting about victims as part of the extortion process.

We then identified the date of each attack as the first day that a victim was posted to a group's leak site. We conceptualize this date as the first date of the attack, although the initial point at which a victim's system was compromised may be several days earlier. Second, we classify each victims within one of fourteen sectors that include commodities (energy, materials), manufactured goods (consumer staples, consumer discretionary goods, industrials), and services (communication, education, financials, health care, information technology, public administration, real estate, utilities).[9] Third, we identified the country in which each victim was located or headquartered based on its website.[10] Accordingly, Figure 2 shows the number of victims by country (4a) and the number of victims divided by each country's Gross Domestic Product (GDP) per capita (4b). These maps show that a majority of victims were in the U.S. (2,048), followed by Canada (231), the UK (200), France (192), Germany (183), and Italy (165) and that the U.S. remains an outlier in terms of its number of victims even after accounting for countries' economic output. Fourth and last, we matched our dataset with information about company size (total assets and number of employees) from Bureau van Dijk's Orbis global database, Compustat North America by Standard & Poor's, and Worldscope by Thomson Financial (see Appendix B.1 for more details).

3.1 Russia-Based Groups

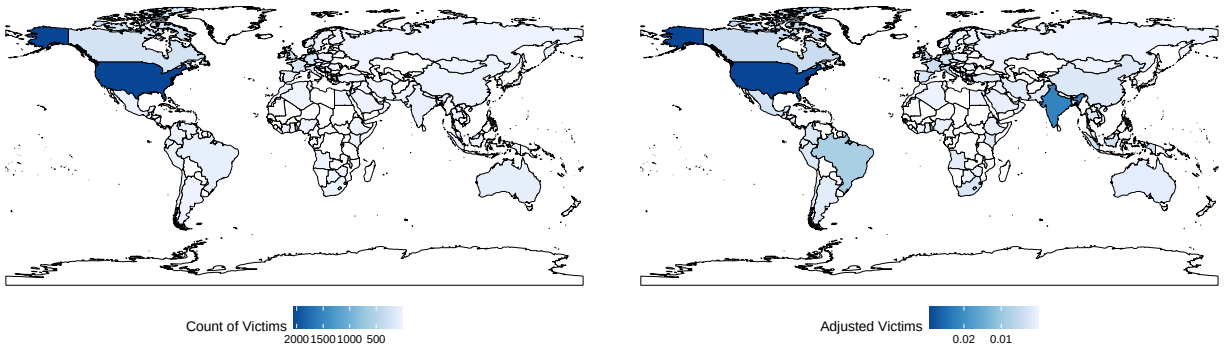
To enable comparisons between Russia-based groups and other groups, we classify each of the 55 groups in our dataset according to whether a group is believed to have core members operating from within Russia. For simplicity, I refer to these groups as Russia-based groups

[9] See Appendix C.

[10] We did not classify a small number of victims with headquarters across multiple countries.

Figure 2: Victims by Country

(a) Total Victims (b) Victims Divided by GDP



Notes: Maps show the number of ransomware victims by country (2a) and the number of victims by country divided by Gross Domestic Product (GDP) per capita (2b) using data from The World Bank (2021). The maps show that even after accounting for the size of a company's economy, the U.S. remains a major outlier in terms of the number of victims.

throughout the remainder of the analysis, although these groups may have some members that operate from other territories. We make this classification based on information from prominent cybersecurity firms and U.S. government reports (see Appendix A). Importantly, we do not assume a group has core members operating in Russia simply because the group communicates in Russian, as many Eastern Europeans communicate in a Russian dialect. We identify eight groups that are believed to have core members operating from within Russia, which account for 1,784 (42.6%) of all victims. One other group in the dataset has ties to another state actor, Pay2Key which is linked to the Iranian government and has carried out attacks against Israeli companies (Gatlan 2020); however, Pay2Key attacked only nine victims. Table 7 presents descriptive statistics for the number of victims by group for Russia-based and other groups.

One potential confounding factor for our analysis lies in the fact that some groups – including both Russia-based and other groups – operate according to a "Ransomware as a Service" (RaaS) model. Because developing encryption malware is a technically sophisticated

Table 1: Descriptive Statistics for Russia-Based and Other Groups

Victims by group	**Min**	**Max**	**Mean**	**Median**	**SD**	***N***
Other Groups	1	494	57.2	30.5	94.9	2,404
Russia-Based Groups	12	842	223	131	263	1,784

Notes: Descriptive statistics include the minimum, maximum, mean, median, standard deviation and count (N) of the number of victims by group for both types of groups.

task, some groups "license" their malware to affiliates who carry out attacks independently and share commissions with the malware-developing group. Thus, successful groups may have multiple affiliates that carry out attacks using their malware; because attribution is typically made on the basis of a ransomware strain, attacks carried out by affiliates are often attributed to the malware-developing group. However, this does not present a problem for our research design, because affiliates are primarily motivated by profit. Thus, affiliate attacks of Russia-based groups are likely to introduce noise to the data that makes detecting a discernible difference between the two types of groups more difficult, thus introducing bias *against* finding an effect.

Table 2 shows the total number of victims by country for all Russia-based and other groups, along with the results of a χ^2 test of the null hypothesis that there is no difference in the proportion of victims from each country for both types of groups. For both types of groups, the majority of victims were located in the U.S. and other major Western democracies. However, Russia-based groups targeted a higher proportion of victims in Canada, Germany, the UK, and the U.S. along with a higher proportion of victims in democracies than other groups. Further, there was only one attack (0.03% of all attacks) against a victim in the Commonwealth of Independent States (CIS), a regional organization made up of former Soviet states. Thus, ransomware groups have largely avoided targeting victims in Russia's sphere of influence while targeting victims in countries Russia views as key adversaries (Bērziņš 2016). We also use a χ^2 test to evaluate differences in the proportion of victims by sector between Russia-based and other groups, and we find that there are few

significant differences between the two types of groups (Appendix C).

Table 2: Victims by Country for Russia-Based and Other Groups

	Other Groups		Russia-Based		χ^2	p-value
	N	(%)	N	(%)		
USA	1,054	46.4	989	57.7	49.48	0.000
Canada	110	4.85	120	7.01	7.97	0.005
France	110	4.85	82	4.79	0.00	0.991
UK	91	4.01	109	6.37	10.86	0.001
Germany	87	3.83	96	5.60	6.59	0.010
Italy	107	4.71	58	3.39	4.01	0.045
Democracies	2,108	92.9	1,675	97.8	48.49	0.000
Total	2,270		1,713			

Notes: Table shows the number of victims by country for all Russia-based and other groups. Values in the last two columns show the result of a χ^2 test of the null hypothesis that there is no difference in the proportion of victims from each country for both types of groups. Russia-based groups attack a higher proportion of victims in Canada, Germany, the UK, the U.S., and democracies than other groups but attack a lower proportion of victims in Italy than other groups. Countries are categorized as democracies using data from Marshall, Gurr, and Jaggers (2019).

4 Targeting of Ransomware Attacks

4.1 Frequency of Attacks Before Elections

To test whether Russia-based groups increase attacks before elections, we measure the frequency of attacks across Canada, Germany, the UK, and the U.S. during national elections. We use the G7 countries as the basis for our sample, as they account for the majority of victims (75%) in our dataset. However, we exclude Japan from our sample as it only had 20 attacks during the six months before and after its election, suggesting that ransomware did not function as a potential vector of electoral interference. We also exclude France because its election occurred after Russia's invasion of Ukraine, which led to a substantial decrease in

the number of attacks globally (see Section 4.2). Lastly, we exclude Canada's federal election on September 20, 2021, as it was a "snap" election that was announced just one month in advance (Cecco 2021). Thus, we analyze attacks before four national elections held between 2019 and 2021 in Canada, Germany, the UK, and the U.S. (Table 3).

Table 3: National Elections Included in Sample

Country	**Date**	**Election Type**
Canada	October 21, 2019	Federal
Germany	September 26, 2021	Federal
UK	December 12, 2019	General
USA	November 3, 2020	Presidential

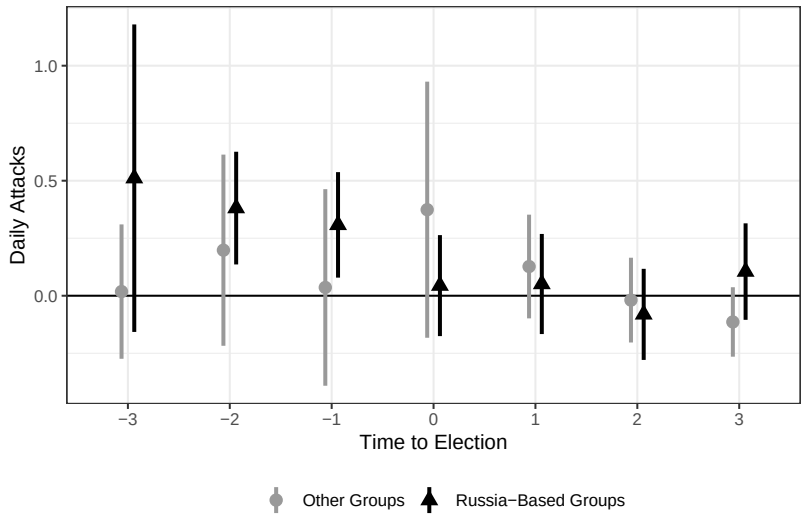
To estimate the relationship between the number of attacks and elections, we create symmetrical samples of the six months before and after a national election for each country and estimate a stacked event study model.[11] Accordingly, our identification strategy allows us to exploit the fact that countries hold elections at different times by identifying electoral cycle effects while controlling for specific time trends. We estimate the following model:

$$\text{Daily Attacks}_{tj} = \alpha_0 + \sum_{p=-3}^{3} \mathbb{1}[\text{Time to Election}_t = p] \times \beta_p + \delta \text{Time}_t + \gamma_j + \epsilon_{tjp}, \quad (1)$$

where *Daily Attacks* specifies the number of daily attacks in a given country (j) on a given day (t). We are primarily interested in the estimates of β_p, which is the effect of being in one of the periods preceding or following the election, or during the election period itself (which we define as the two weeks surrounding the election) on the expected number of daily ransomware attacks. *Time to Election*, is defined as the three months preceding and following a two week period around election day. We also include a time linear variable at the month-year level (δ) to capture time trends and country fixed effects (γ) to account for differences in the number of attacks by country. We estimate the model twice: once for the

[11] The stacked event study model was first introduced in Deshpande and Li (2019) and Cengiz et al. (2019). Wing (2021) describes the method.

Figure 3: Daily Attacks and Time to Election for Russia-based and Other Groups



Notes: Plot presents coefficients and confidence intervals (with robust standard errors) for the effect of being in one of the three months before or after an election period (which we define as the two weeks around the election) on the expected number of daily ransomware attacks by Russia-based (black) and other (gray) groups. It shows a statistically significant increase in the expected number of daily attacks by Russia-based groups two and one month before an election period, with no change in the expected number of daily attacks by other groups

number of attacks by Russia-based groups and again for the number of attacks by other groups.

Figure 3 shows a plot of the coefficients and confidence intervals for the effect of being in a period close to an election on the number of ransomware attacks, with estimates for Russia-based and other groups presented separately (Equation 1). While there is no clear pattern to the number of attacks by other groups in the periods surrounding an election, there is a statistically significant *increase* in the expected number of daily attacks by Russia-based groups before elections. This effect is meaningful in substantive terms – equal to a roughly 30% increase in the expected number of daily attacks by Russia-based groups one and two months before an election period. Thus, the results show an increase in attacks by Russia-based groups before elections, with no similar increase in attacks by other groups.

This diverging behavior between Russia-based and other groups is consistent with the

possibility that additional motives *beyond financial ones* are at play. If groups carried out more attacks before elections because they found victims were more likely to pay, then we would expect to see a similar increase in attacks by other groups. To gain insight into what drives the increase in attacks by Russia-based groups, we estimate the number of attacks before elections disaggregated by sector (Appendix D.3); we find a statistically significant increase in the number of attacks before an election across across eight out of fourteen sectors, including government, health care, financial services, and energy, as well as manufacturing sectors (consumer discretionary, consumer staples, industrials, and materials). This suggests that a focus on election infrastructure *alone* is unlikely to explain increased attacks, as other sectors beyond government alone were targeted.

To test the robustness of these findings, we estimate alternate specifications of our main model. First, we estimate the model with the outcome coded as a binary variable indicating whether there was at least one attack on a given day; once again, we find an increase in attacks by Russia-based groups before elections (with no similar increase in attacks by other groups) (Appendix D.2). Next, we estimate a similar model using a separate data source – the number of payments made to ransomware groups before elections in a dataset by crypto-analytic company Chainalysis (Appendix E). Because we do not know the location of the senders behind these payments, we cannot estimate country-specific models; instead, we estimate the frequency of payments sent before three U.S. national elections (2016, 2018, and 2020), as the U.S. accounted for the majority of victims in the dataset. We find a statistically significant increase in the number of payments going to Russia-based ransomware groups (but not other groups) before elections. Thus, we find similar results using different specifications of the model and different data sources, underscoring the robustness of our findings.

4.2 Frequency of Attacks After the Invasion

We also measure the frequency of ransomware attacks after the invasion, which we argue provides insight into the relationship between Russia's official cyber forces and ransomware

groups. To measure how the invasion impacted the frequency of ransomware attacks, we regress a dummy variable for dates after the invasion on the number of daily attacks by all ransomware groups. We estimate the following model:

$$\text{Daily Attacks}_{itm} = \beta_0 + \beta_1 \text{Invasion} + \beta_2 \text{Time}_t + \kappa_m + \epsilon_{itm}, \tag{2}$$

where i is the day, t is the month-year, and m is the month of an attack. Results in Table 4 show a statistically significant *decrease* in the expected number of daily ransomware attacks in the months after the invasion (equal to roughly two fewer attacks per day); this finding is robust to the inclusion of both month fixed effects and a month-year linear trend. This finding is counter to warnings from the U.S. government that Russia might *increase* ransomware attacks and other cyber attacks after the invasion as it faced increasing economic pressure caused by sanctions (The White House 2022). Instead, we argue that the decrease in attacks after the invasion is consistent with the possibility of a *substitution effect* in Russia's cyber activity.

A decrease in ransomware attacks after the invasion is consistent with the possibility that the Russian government recruited ransomware operators to fill the ranks of its official cyber forces, as the invasion increased government demand for skilled cyber actors that could mount a cyber offensive against Ukraine (Google 2023, pp. 6–27).[12] Indeed, Russia has recruited cybercriminals to carry out other state missions (U.S. Department of Justice 2017), and there is evidence that former members of ransomware group Conti have joined Russian government forces waging cyber attacks against Ukraine (Villadsen, Hammond, and Weinberger 2022; Google 2023, p. 44). Further, tools from Conti and another Russia-based ransomware group, Cuba, have been re-purposed to aid the Russian government's cyber offensive against Ukraine, showing connections between ransomware groups and the Russian government (Google 2023, p. 44). Thus, by allowing ransomware groups to operate from within its borders, Russia receives an important benefit: access to a pool of specialized

[12]We address two alternate explanations in Appendix F.

Table 4: Frequency of Attacks Post Invasion

	Number of Daily Attacks		
	(1)	(2)	(3)
Post Invasion	-2.090^{***}	-1.293^{**}	-2.164^{**}
	(0.355)	(0.443)	(0.769)
Constant	4.259^{***}	5.016^{***}	4.170^{***}
	(0.208)	(0.558)	(0.583)
Month FEs			✓
Month-year (Linear)		✓	✓
Observations	698	698	698
R^2	0.006	0.006	0.037
Adjusted R^2	0.005	0.003	0.019

Notes: Dependent variable is the number of daily ransomware attacks. The primary independent variable is a dummy variable indicating dates *after* Russia's invasion of Ukraine. Robust standard errors are in parentheses. Stars indicate the statistical significance level: $^{*}p<0.05$; $^{**}p<0.01$; $^{***}p<0.001$.

cyber talent available for recruitment.[13]

4.3 Targeting Companies that Condemned the Invasion

Lastly, we test whether companies that withdrew or suspended operations in Russia after the invasion were more likely to become a victim of ransomware. To identify companies that withdrew or suspended operations in Russia after the invasion, we use a list compiled by Yale University's Chief Executive Leadership Institute (CELI). CELI assigned A-F letter grades to over 1,200 companies based on how each company responded to the invasion, with higher grades going to companies that took more aggressive actions to limit their activities in Russia (Yale School of Management n.d.). The CELI list received widespread media attention – increasing the visibility of companies' actions and the salience of these choices as a political response to the invasion; further, some companies' withdrawals were highly visible, such as McDonald's closure of 800 locations across Russia (Jan 2022; Creswell 2022). Thus, a company's decision to withdraw or suspend operations in Russia was both highly visible and widely perceived as political.

To test this, we identified all companies (and their subsidiaries) from the CELI list that are included in our dataset. We estimate the following model:

$$\begin{aligned} \text{Daily Attacks}_{mti} = \beta_0 + \beta_1 \text{Invasion}_i + \beta_2 \text{A/B Companies} + \\ \beta_3 \text{Invasion} \times \text{A/B Companies} + \beta_4 \text{Time}_t + \delta_m + \epsilon_{mti}, \end{aligned} \tag{3}$$

where i is the day, t is the month-year, and m is the month of an attack. The outcome variable is the number of daily ransomware attacks between May 1, 2020 and April 30, 2022. There are two independent variables – one is an indicator of attacks against A or B rated companies and one identifies dates following the invasion. We are primarily interested in β_3, which is the interaction between an indicator of A or B rated companies and the post-invasion period. We also include a month-year linear time trend (β_4) and fixed effects by

[13]This is a potential benefit identified by Egloff (2022, pp. 91–92).

month of the attack (δ).

Table 5: Daily Attacks Against A/B Rated Companies Post Invasion

	Number of Daily Attacks		
	(1)	(2)	(3)
A/B Companies	-5.267^{***}	-5.498^{***}	-5.498^{***}
	(0.234)	(0.254)	(0.251)
Post Invasion		-2.519^{***}	-3.265^{***}
		(0.431)	(0.567)
Post Invasion × A/B Companies		2.559^{***}	2.559^{***}
		(0.432)	(0.436)
Constant	5.322^{***}	5.550^{***}	4.595^{***}
	(0.233)	(0.253)	(0.461)
Month-year (Linear)			✓
Month FEs			✓
Observations	1,460	1,460	1,460
R^2	0.258	0.267	0.285
Adjusted R^2	0.257	0.266	0.278

Notes: Table shows that there is a positive and statistically significant relationship between the number of daily attacks against A or B rated companies (or their subsidiaries) and post-invasion period. Standard errors are in parentheses. Data on company ratings provided by the Yale CELI list. Robust standard errors are in parentheses, and stars indicate the statistical significance level : $^{***}p<0.001$.

Table 5 shows that A or B rated companies had a greater number of expected daily ransomware attacks following the invasion. Across the full dataset, the expected number of daily ransomware attacks against A or B rated companies is 0.055 (column 1). After the invasion, the expected number of daily ransomware attacks against A or B rated companies increases by 67% over the baseline, representing a substantial increase in risk for these companies. This relationship is robust to the inclusion of a month-year time trend variable and month fixed effects (column 3), and we provide additional robustness tests of this findings

in Appendix G.2. These findings suggest that ransomware groups may have retaliated against companies that withdrew or suspended operations in Russia after the invasion by targeting them with ransomware.

Why might ransomware groups target companies that withdrew or suspended operations in Russia? One possibility is that ransomware groups took the initiative to retaliate against these companies. The idea that patriotic Russian cyber actors might work independently to benefit the Russian government has become popular in the academic scholarship and policy circles,[14] and one ransomware group, Conti, threatened to carry out cyber attacks against any entity that attacked the Russian Federation following Russia's invasion of Ukraine (Bing 2022). Although possible, it is notable that the few known cases in which a ransomware group considered political operations (discussed in the next section) were the result of members' connections to the government rather than the group's own initiative. Another possibility is that the Kremlin may have encouraged ransomware groups to target certain companies by, for example, sharing a list of targets. However, without further evidence, it is unclear what factor or factors led A or B rated companies to be more likely to experience a ransomware attack after the invasion.

5 Insights from One Group's Internal Communications

To further probe Russia's relationship to ransomware groups, we analyze leaked chat logs from a prolific Russia-based ransomware group, Conti. Conti attacked over 1,000 victims (including 842 in our dataset) over two years and received at least $150 million in ransom payments, leading the U.S. Department of State to describe it as the "costliest strain of ransomware ever documented" (Price 2022). Although the group's leadership had connections to the Kremlin, Conti drew members from across Eastern Europe, some of whom opposed Russia's invasion of Ukraine; the group fell apart in the months following the invasion. We

[14] See for example Dinniss (2013), Lokot (2017), Hare (2019), and Conduit (2023).

structure our analysis of the chat logs around three themes: the group's structure and daily operations, Russia's provision of safe harbor to ransomware groups, and connections between the Conti and the Kremlin.

5.1 Is Conti structured like an apparatus of the state or a criminal group?

The chats reveal that Conti was first and foremost a *criminal organization* that operated independently from the Russian government and its array of state-backed cyber units. Unlike other Russian cyber proxies such as Cozy Bear and Fancy Bear, which are affiliated with the Federal Security Service (FSB) and the military intelligence agency (GRU) respectively, Conti possessed its own chain of command and primarily focused on criminal rather than state missions. Conti was structured hierarchically with one boss at the top who oversaw a handful of mid-level managers, who, in turn, oversaw teams with dozens of members. Like other criminal and violent groups, Conti adopted bureaucratic methods from legitimate businesses to run its operations (Levitt and Venkatesh 2000; Lessing and Willis 2019; Johnston et al. 2016), including paying members on the first and fifteenth of each month and scanning legitimate job boards for tech savvy candidates to recruit (Krebs 2022). Conti's legitimate business practices only extended so far, however, as the group often missed payments for business expenses and failed to inform some new recruits that they were joining a criminal organization, posing instead as a legitimate business.

Many of the group's day-to-day discussions focus on a key operational task – negotiating ransoms with victims. Members engaged in extensive internal discussions during negotiations and used public information about their victims (including company financial information) to set custom ransom demands. Conti leaders guided lower-level members in how to increase pressure on their victims, instructing them to search for sensitive financial documents within a victim's compromised computer system. Although it is unclear how Conti selected victims for attack, these discussions reveal that members' primary objective during negotiations was

to obtain the largest ransom possible, underscoring that most members' actions appear to have been motivated by financial gain rather than any type of politics.

5.2 Chat logs reveal Conti members believe Russia provides safe harbor

The chat logs reveal that group members believed they were safe from foreign prosecution as long as they remained in Russia. At one point, a group member named Skippy (all group members went by pseudonyms) discussed his plans to vacation abroad with his boss, Mango. "All of the special services of the world are looking for us," Mango cautions. "They can pull from any country," he writes, referencing the United States' extradition access. When Skippy shares that he still plans to travel, Mango provides tips including traveling without a laptop, deleting content from one's phone, and buying an airline ticket "on the spot." This exchange highlights that group members were aware of the potential legal jeopardy they faced when traveling abroad.

The chats also show that group members did not view Russia's arrest of members of another ransomware group, REvil – the only known case in which Russia has arrested ransomware operators – as a serious threat. Instead, Conti members reacted casually to the news, with one noting that the FSB does not cooperate with the U.S. and writing that the FSB would allow the arrested group members "to rest, regroup and [return] with renewed vigor." This stands in sharp contrast to how members reacted to *foreign* investigations and arrests of ransomware operators, which the group closely monitored. Thus, Conti members' reactions to Russia's first known arrests of ransomware operators suggests that they viewed the arrests as a temporary obstacle rather than a meaningful step toward judicial accountability for cybercriminals.

5.3 Chat logs show ties with Kremlin

The chats also reveal evidence of direct contact and cooperation between Conti members and the Kremlin. In one instance, a government official shared information about an ongoing law enforcement investigation. A Conti member wrote that his contact had informed him that the Russian government had reopened an investigation into the group. The Russian government reopened the case because the Americans had been requesting more information about Russian hackers, and specifically, which ransomware operators had been caught in the country. The member went on to write that Conti members should lay low until the end of October 2021, when his contact suspected the case would no longer be active. This communication shows that Conti received valuable information from the Russian government – details about an ongoing foreign-led investigation – that helped protect group members.

In another instance, Conti's leaders discussed activities by Russian state-backed hackers and opportunities for the group to collaborate with them. During the COVID-19 pandemic, a Russian state-backed hacking group called Cozy Bear carried out cyberattacks against vaccine researchers in Canada, the UK, and the U.S., likely aimed at gathering intelligence (Gallagher 2020). Two Conti members, Stern and his boss Professor, discussed Cozy Bear's activities; both members had been (independently) solicited by government contacts with propositions to help Cozy Bear carry out attacks against its list of targets. Professor asked Stern whether his contact would pay Conti for its help, or if the group was asked to carry out attacks for free as a patriotic favor to the government.[15] Professor then shared that his contact had offered to pay for each victim Conti attacked, and although the pay would not be high, establishing a stable relationship with his contact would ensure that Conti would receive help if it ran into trouble in the future. Professor and Stern then discussed setting up a separate division within Conti to handle political operations.

[15]Specifically, Professor asked Stern if his contact would pay for their help or if they would be "playing Pioneers," a reference to the Soviet Union's Young Pioneers youth organization.

In a similar vein, another exchange shows that Conti helped a government contact hack a foreign journalistic organization. Mango, the mid-level manager, tells Professor that he received a request from one of his contacts for help targeting "people who work against the Russian Federation." Mango asks Professor whether Conti will "work on politics," or if they should focus on crime and avoid "political fuss." "Yes, we are patriots," Professor replies, authorizing Conti's involvement in the hack. Mango then helped his contact target Bellingcat, an journalistic organization headquartered in the Netherlands; his contact was interested in Bellingcat's investigation into Russian opposition leader Alexy Navalny's poisoning, which Western intelligence and Bellingcat attributed to the FSB. Bellingcat has since stated that Mango's contact was most likely an FSB officer, as Bellingcat had previously received a tip that the FSB was partnering with a criminal group to hack them (Burges 2022).

These interactions show that the Kremlin shared information with Conti's leaders, and Conti's leaders reciprocated by performing at least one targeted cyber attack against a foreign entity. They also show that multiple Conti leaders had contacts in the government, and the cases of cooperation that developed between them appear to have been largely *ad hoc* and informal. Conti members also did not fear arrest by Russian government officials, and, by contrast, members maintained open lines of communications with contacts inside the government.

6 Discussion and Conclusion

In this paper, we have sought to understand the relationship between Russia and Russia-based ransomware groups. Based on our analysis of a dataset of ransomware victims and one group's internal communications, we argue that the Russian government maintains a cooperative yet informal relationship with ransomware groups. Indeed, Conti's relationship with the Kremlin was decentralized (as multiple Conti leaders were in touch with government contacts), and the nature of their discussions with these contacts appears to have been

informal. Below, we explore one key benefit that Russia provides – safe harbor – and three benefits that ransomware groups provide – plausible deniability, access to specialized skills, and targeting of Russia's enemies – as part of this relationship.

6.1 Safe Harbor

The primary benefit Russia provides ransomware groups is protection from domestic and foreign prosecution. Although many Eastern European countries previously showed lax enforcement of laws around cybercrime (Kostyuk and Geers 2015), several of these countries have cooperated with Western law enforcement in recent years to arrest ransomware operators and other cybercriminals operating from within their borders.[16] Russia has also continued to provide safe harbor despite facing increasing international pressure on this issue from the U.S., the G7, and other Western countries (Doherty 2021; Palmer 2021).

Not only has Russia refused to cooperate with Western law enforcement, it has sometimes actively undermined their investigations by sharing information with targets under investigation. Our analysis shows that Russian officials shared information with ransomware group Conti about a U.S.-led investigation, providing the group with intelligence that helped its members avoid arrest. Experts also suspect that Russia uses information shared by foreign enforcement agencies to identify cybercriminals for recruitment.[17] However, we *do not* find evidence that the Russian government has provided significant material benefits to groups. We conclude this based on the fact that there is no statistically significant difference in the size of victims targeted by Russia-based and other ransomware groups, as groups with greater capabilities typically target larger victims (Appendix B). Further, Conti's internal discussions reveal that group members did not expect to receive much pay in exchange for help provided to government contacts.

[16]See for example Cimpanu (2022), Cimpanu (2021a), Cimpanu (2021c), Page (2023), Interpol (2021), and Cimpanu (2021b).

[17]See for example Stubbs (2017) and Collins (2017).

6.2 Plausible Deniability

We argue that the Kremlin benefits from its relationship with ransomware groups by obtaining plausible deniability. Specifically, by engaging ransomware groups to carry out certain state-backed activities, Russia blurs the line between government and criminal activities and makes attribution more difficult. We see this in Conti's hack of Bellingcat, as Conti's involvement created ambiguity about the nature of the actors involved and their motives. And although it is unclear whether they followed through, group members discussed attacking targets on a government-generated list of companies researching a COVID-19 vaccine. In both instances, the Russian government sought to involve Conti in politically sensitive missions targeting foreign entities.

Another context in which Russia may seek plausible deniability is that of ransomware attacks before elections. Specifically, we find an increase in the number of ransomware attacks by Russia-based groups before elections across several major democracies, with no similar increase in attacks by other groups. Although there is no evidence that the Russian government has directed or encouraged these attacks, U.S. government officials warn that "malicious threat actors" could use ransomware to disrupt elections (FBI & CISA 2022). Thus, potential election meddling through ransomware remains an ongoing area of concern for Western countries.

6.3 Access to Cyber Talent

Russia also benefits from its relationship with ransomware groups by obtaining access to a pool of specialized cyber actors that it can recruit for state operations. Indeed, ransomware groups have managed to develop sophisticated cyber skills while attacking foreign companies and governments. By contrast, developing a technologically skilled workforce through legal means requires governments to secure significant public and private investment, something the government has largely failed to deliver. Thus, the Russian government has managed

to overcome its failure to develop human capital by recruiting from the ranks of skilled cybercriminals.

We see this dynamic most clearly in the wake of the invasion, which increased Russia's demand for skilled cyber actors to carry out attacks against Ukraine (Google 2023). Notably, we find a decrease in the number of ransomware attacks after the invasion, which we argue is likely driven by Russia's recruitment of ransomware operators. Indeed, Conti's top boss disappeared just days before the invasion, and although it is unclear why, one possible explanation is that he was recruited to aid the government offensive. Thus, Russia's recruitment of former ransomware operators and its re-purposing of tools from ransomware groups highlights the porous nature of the relationship between ransomware groups and Russia's official cyber forces.

6.4 Harm to Adversaries

Lastly, we argue that Russia has benefited indirectly from destruction wrought against its adversaries by ransomware attacks. As shown throughout this paper, groups have overwhelmingly targeted victims in countries that are Russian rivals while avoiding victims in its sphere of influence. Although there is no evidence that Russia has encouraged ransomware groups to target victims in certain countries, we argue that Russia likely views the damage caused by these attacks as a strategic advantage. Specifically, Russia's foreign policy seeks to weaken Western alliances and destabilize civil society in the U.S. and major European countries. In pursuit of these goals, Russia employs a decentralized approach by engaging a wide range of public and private actors, with each acting in her own capacity to help achieve these objectives (Chivvis 2017; McKew 2017). Thus, although there is no direct evidence that Russia encourages groups to target certain countries, its past actions suggest that it likely views these attacks as a boon to its geopolitical agenda.

In this paper, we have sought to shed light on the relationship between the Russian government and ransomware groups. We analyzed an original dataset of ransomware attack

victims and leaked internal communications from a major ransomware group. We find that the Russian government appears to provide protection to ransomware groups, although it appears to stop short of providing significant material support. The Russian government, in turn, benefits from services ransomware groups provide, as well as their ability to specialize in relevant cyber skills. We also find evidence suggestive of political (in addition to financial) motivations behind these attacks, including an increase in attacks by Russia-based groups before elections and the fact that companies that withdrew or suspended operations in Russia after the invasion were more likely to be targeted with ransomware.

These findings highlight that ransomware is not only a form of crime, it is also an international security threat – and particularly in the context of attacks originating from groups in Russia. Accordingly, one of the biggest challenges in combating ransomware lies in addressing Russia's provision of safe harbor to ransomware groups. Although diplomacy between Russia and the West has largely broken down during the conflict in Ukraine, Western countries can continue to push for accountability by developing an international norm that states should not shelter cybercriminals from international prosecution. Thus, countries must address the international dimensions of this challenge to hold ransomware operators responsible for their destructive attacks.

References

Abrams, Lawrence (2021). "Ransomware gang threatens to wipe decryption key if negotiator hired". In: URL: https://www.bleepingcomputer.com/news/security/ransomware-gang-threatens-to-wipe-decryption-key-if-negotiator-hired/.

Akoto, William (2022). "Accountability and cyber conflict: examining institutional constraints on the use of cyber proxies". In: *Conflict Management and Peace Science* 39.3, pp. 311–332.

Al-Tamimi, Aymenn (2015). "The evolution in Islamic State administration: The documentary evidence". In: *Perspectives on Terrorism* 9.4, pp. 117–129.

Albarracín, Juan (2018). "Criminalized electoral politics in Brazilian urban peripheries". In: *Crime, law and social change* 69, pp. 553–575.

Arias, Enrique Desmond (2006). "The dynamics of criminal governance: networks and social order in Rio de Janeiro". In: *Journal of Latin American Studies* 38.2, pp. 293–325.

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, Nicholas (2017). "Criminal politics: An integrated approach to the study of organized crime, politics, and violence". In: *Perspectives on Politics* 15.4, pp. 967–987.

Bērziņš, Jānis (2016). "The West is Russia's Main Adversary, and the Answer is New Generation Warfare". In: *Sicherheit und Frieden (S+ F)/Security and Peace*, pp. 171–176.

Bing, Christopher (2022). "Russia-based ransomware group Conti issues warning to Kremlin foes". In: URL: https://www.reuters.com/technology/russia-based-ransomware-group-conti-issues-warning-kremlin-foes-2022-02-25/.

Bing, Christopher and Raphael Satter (2019). "Louisiana government computers knocked out after ransomware attack". In: 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 (2016). "Can states calculate the risks of using cyber proxies?" In: *Orbis* 60.3, pp. 395–416.

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

— (2023). "China Is Relentlessly Hacking Its Neighbors". In: *WIRED*. URL: https://www.wired.com/story/china-hack-emails-asean-southeast-asia/.

Caesar, Ed (2021). "The Incredible Rise of North Korea's Hacking Army". In: *The New Yorker* 26.

Cecco, Leyland (2021). "Justin Trudeau secures a third victory in an election 'nobody wanted'". In: *The Guardian*. URL: https://www.theguardian.com/world/2021/sep/21/justin-trudeau-wins-third-election-victory.

Cengiz, Doruk et al. (2019). "The effect of minimum wages on low-wage jobs". In: *The Quarterly Journal of Economics* 134.3, pp. 1405–1454.

Cerulus, Laurens (2020). "US calls out Russia for Macron campaign hack, even as France stays silent". In: *Politico*. URL: https://www.politico.eu/article/us-russia-macron-campaign-hack-2017-election-france-attribution-gru/.

Chivvis, Christopher S (2017). "Understanding Russian "Hybrid Warfare"". In: *Rand Corporation* 17.

Cimpanu, Catalin (2021a). "Arrested Clop gang members laundered over $500M in ransomware payments". In: URL: https://therecord.media/arrested-clop-gang-members-laundered-over-500m-in-ransomware-payments.

— (2021b). "Egregor ransomware operators arrested in Ukraine". In: URL: https://www.zdnet.com/article/egregor-ransomware-operators-arrested-in-ukraine/.

Cimpanu, Catalin (2021c). "Europol detains suspects behind LockerGoga, MegaCortex, and Dharma ransomware attacks". In: URL: https://therecord.media/europol-detains-suspects-behind-lockergoga-megacortex-and-dharma-ransomware-attacks.

— (2022). "Ransomware gang behind attacks on 50 companies arrested in Ukraine". In: URL: https://therecord.media/ransomware-gang-behind-attacks-on-50-companies-arrested-in-ukraine.

CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK, and the UK National Crime Agency (NCA) (2022). "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure". In: URL: https://www.cisa.gov/uscert/sites/default/files/publications/AA22-110A_Joint_CSA_Russian_State-Sponsored_and_Criminal_Cyber_Threats_to_Critical_Infrastructure_4_20_22_Final.pdf.

Cohen, Julie E (2007). "Cyberspace as/and Space". In: *Colum. L. Rev.* 107, p. 210.

Collier, Kevin (2022). "Russia arrests ransomware gang responsible for high-profile cyberattacks". In: URL: https://www.nbcnews.com/tech/security/russia-arrests-ransomware-gang-responsible-high-profile-cyberattacks-rcna12235.

Collins, Keith (2017). "Russia is recruiting the FBI's most-wanted hackers". In: URL: https://qz.com/934432/russian-intelligence-recruited-alexsey-belan-and-evgeniy-bogachev-fbis-most-wanted-hackers.

Conduit, Dara (2023). "Digital authoritarianism and the devolution of authoritarian rule: examining Syria's patriotic hackers". In: *Democratization*, pp. 1–19.

Council on Foreign Relations (2021). "Cyber Operations Tracker". In: URL: https://www.cfr.org/cyber-operations/.

Creswell, Julie (2022). "McDonald's, Coca-Cola and Starbucks temporarily stop sales in Russia." In: *The New York Times*. URL: https://www.nytimes.com/2022/03/08/business/mcdonalds-russia.html.

Cybereason (2022). "RansomOps: Inside Complex Ransomware Operations and the Ransomware Economy". In: URL: https://www.cybereason.com/blog/white-paper-inside-complex-ransomops-and-the-ransomware-economy.

Dal Bó, Ernesto, Pedro Dal Bó, and Rafael Di Tella (2006). ""Plata o Plomo?": bribe and punishment in a theory of political influence". In: *American Political science review* 100.1, pp. 41–53.

Dark Tracer Intelligence (2021). *Intelligence Report on Ransomware Gangs on the Darkweb*. URL: https://twitter.com/stealthmole_int/status/1394189875096657921.

De Feo, Giuseppe and Giacomo Davide De Luca (2017). "Mafia in the ballot box". In: *American Economic Journal: Economic Policy* 9.3, pp. 134–167.

Deshpande, Manasi and Yue Li (2019). "Who is screened out? Application costs and the targeting of disability programs". In: *American Economic Journal: Economic Policy* 11.4, pp. 213–248.

Dinniss, Heather Harrison (2013). "Participants in Conflict–Cyber warriors, patriotic hackers and the laws of war". In: *International Humanitarian Law and the Changing Technology of War*. Brill Nijhoff, pp. 251–278.

Dipoppa, Gemma (2021). "How criminal organizations expand to strong states: Migrant exploitation and political brokerage in Northern Italy". In.

DiResta, Renée, Shelby Grossman, and Alexandra Siegel (2022). "In-house vs. outsourced trolls: How digital mercenaries shape state influence strategies". In: *Political Communication* 39.2, pp. 222–253.

Doherty, Erin (2021). "White House says Biden warned Putin on ransomware attacks". In: URL: https://www.axios.com/2021/07/09/white-house-says-biden-warned-putin-on-ransomware-attacks.

Dube, Arindrajit, Oeindrila Dube, and Omar García-Ponce (2013). "Cross-border spillover: US gun laws and violence in Mexico". In: *American Political Science Review* 107.3, pp. 397–417.

Egloff, Florian J (2022). *Semi-State Actors in Cybersecurity*. Oxford University Press.

FBI & CISA (2022). "Malicious Cyber Activity Against Election Infrastructure Unlikely to Disrupt or Prevent Voting". In: URL: https://www.cisa.gov/sites/default/files/2023-01/psa_cyber-activity_508.pdf.

Field, Matthew (2023). "Russia-linked Lockbit hackers threaten to publish Royal Mail data". In: URL: https://www.telegraph.co.uk/business/2023/02/07/russia-linked-lockbit-ransomware-hacking-gang-threatens-publish/.

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

Gallagher, Ryan (2020). "'Cozy Bear' Group Tied to Hacks on Covid Vaccine Research". In: *Bloomberg*. URL: https://www.bloomberg.com/news/articles/2020-07-16/low-profile-cozy-bear-tied-to-hacks-on-covid-vaccine-research.

Gambetta, Diego (1993). "The sicilian mafia". In: *TLS-THE TIMES LITERARY SUPPLEMENT* 4724, pp. 15–15.

Gatlan, Sergiu (2020). "Iranian nation-state hackers linked to Pay2Key ransomware". In: URL: https://www.bleepingcomputer.com/news/security/iranian-nation-state-hackers-linked-to-pay2key-ransomware/.

— (2021). "Ukraine arrests Clop ransomware gang members, seizes servers". In: URL: https://www.bleepingcomputer.com/news/security/ukraine-arrests-clop-ransomware-gang-members-seizes-servers/.

Google (2023). "Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape". In: URL: https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

Hare, Forrest B (2019). "Privateering in cyberspace: should patriotic hacking be promoted as national policy?" In: *Asian Security* 15.2, pp. 93–102.

Health Sector Cybersecurity Coordination Center (2023). "HC3: Analyst Note". In: URL: https://www.hhs.gov/sites/default/files/clop-ransomware-analyst-note-tlpclear.pdf.

Hope, Alicia (2021). "FBI Warns That Cuba Ransomware Gang Made $44 Million After Compromising 49 Critical Infrastructure Entities in Five Sectors". In: *CPO Magazine*. URL: https://www.cpomagazine.com/cyber-security/fbi-warns-that-cuba-ransomware-gang-made-44-million-after-compromising-49-critical-infrastructure-entities-in-five-sectors/.

Human Rights Watch (2022). "Iran: State-Backed Hacking of Activists, Journalists, Politicians". In: *The Intercept*. URL: https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians.

Hussain, Murtaza (2023). "The Grisly Cult of the Wagner Group's Sledgehammer". In: *The Intercept*. URL: https://theintercept.com/2023/02/02/wagner-group-violence-sledgehammer/.

Ilascu, Ionut (2020). "FIN11 hackers jump into the ransomware money-making scheme". In: URL: https://www.bleepingcomputer.com/news/security/fin11-hackers-jump-into-the-ransomware-money-making-scheme/.

— (2021). "DoppelPaymer ransomware gang rebrands as the Grief group". In: URL: https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-gang-rebrands-as-the-grief-group/.

Interpol (2021). "Ransomware gang arrested in Ukraine". In: URL: https://www.interpol.int/en/News-and-Events/News/2021/Ransomware-gang-arrested-in-Ukraine.

Jan, Tracy (2022). "How a Yale professor's viral list pressured companies to pull out of Russia". In: *The Washington Post*. URL: https://www-washingtonpost-com.stanford.idm.oclc.org/business/2022/03/11/sonnenfeld-russia-ukraine-corporations/.

Johnston, Patrick B et al. (2016). *Foundations of the Islamic State: management, money, and terror in Iraq, 2005-2010*. Rand Corporation.

Kalemli-Ozcan, Sebnem et al. (2015). *How to construct nationally representative firm level data from the Orbis global database: New facts and aggregate implications*. Tech. rep. National Bureau of Economic Research.

Kostyuk, Nadiya and Kenneth Geers (2015). "Ukraine: A Cyber Safe Haven?" In: *Cyber War in Perspective: Russian Aggression against Ukraine. Tallinn: NATO Cooperative Cyber Defence Centre of Excellence*, pp. 113–122.

Kramer, Andrew E., Michael Schwirtz, and Anton Troianovski (2021). "Secret Chats Show How Cybergang Became a Ransomware Powerhouse". In: *N.Y. Times*. URL: https://www.nytimes.com/2021/05/29/world/europe/ransomware-russia-darkside.html.

Krebs, Brian (2021). "Ukrainian Police Nab Six Tied to CLOP Ransomware". In: URL: https://krebsonsecurity.com/2021/06/ukrainian-police-nab-six-tied-to-clop-ransomware/.

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

Lessing, Benjamin (2015). "Logics of violence in criminal war". In: *Journal of Conflict Resolution* 59.8, pp. 1486–1516.

— (2021). "Conceptualizing criminal governance". In: *Perspectives on politics* 19.3, pp. 854–873.

Lessing, Benjamin and Graham Denyer Willis (2019). "Legitimacy in criminal governance: Managing a drug empire from behind bars". In: *American Political Science Review* 113.2, pp. 584–606.

Levitt, Steven D and Sudhir Alladi Venkatesh (2000). "An economic analysis of a drug-selling gang's finances". In: *The quarterly journal of economics* 115.3, pp. 755–789.

Ley, Sandra (2018). "To vote or not to vote: how criminal violence shapes electoral participation". In: *Journal of Conflict Resolution* 62.9, pp. 1963–1990.

Lokot, Tetyana (2017). "Public Networked Discourses in the Ukraine-Russia Conflict: 'Patriotic Hackers' and Digital Populism". In: *Irish Studies in International Affairs* 28.1, pp. 99–116.

Loui, Eric and Josh Reynolds (2021). "Carbon Spider Embraces Big Game Hunting, Part 1". In: URL: https://www.crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/.

Magaloni, Beatriz, Edgar Franco-Vivanco, and Vanessa Melo (2020). "Killing in the slums: Social order, criminal governance, and police violence in Rio de Janeiro". In: *American Political Science Review* 114.2, pp. 552–572.

Malwarebytes Labs (2021). "Ransomware's Russia problem". In: URL: https://www.malwarebytes.com/blog/news/2021/07/ransomwares-russia-problem.

Markoff, John (2008). "Before the Gunfire, Cyberattacks". In: *The New York Times*. URL: https://www.nytimes.com/2008/08/13/technology/13cyber.html.

Marks, Joseph (2022). "Chinese hackers breached six state governments, researchers say". In: *The Washington Post*. URL: https://www.washingtonpost.com/politics/2022/03/08/chinese-hackers-breached-six-state-governments-researchers-say/.

Marshall, Monty G., Ted R. Gurr, and Keith Jaggers (2019). *Polity IV Project: Political Regime Characteristics and Transitions, 1800-2018. Dataset Users' Manual*. Center for Systemic Peace. URL: http://www.systemicpeace.org/inscr/p4manualv2018.pdf.

Marten, Kimberly (2019). "Russia's use of semi-state security forces: the case of the Wagner Group". In: *Post-Soviet Affairs* 35.3, pp. 181–204.

McKew, Molly K. (2017). "The Gerasimov Doctrine". In: URL: https://www.politico.com/magazine/story/2017/09/05/gerasimov-doctrine-russia-foreign-policy-215538/.

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.

Mueller, Robert S and Man With A. Cat (2019). *Report on the investigation into Russian interference in the 2016 presidential election*. Vol. 1. US Department of Justice Washington, DC.

Nakashima, Ellen and Shane Harris (2018). "How the Russians hacked the DNC and passed its emails to WikiLeaks". In: *The Washington Post*. URL: https://www-washingtonpost-com.stanford.idm.oclc.org/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78_story.html.

Nakashima, Ellen and Tim Starks (2022). "Iranian hackers breached the agency that hears federal worker grievances". In: *The Washington Post*. URL: https://www.washingtonpost.com/politics/2022/11/17/iranian-hackers-breached-agency-that-hears-federal-worker-grievances/.

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.

Nieto-Matiz, Camilo (2022). "When the State Becomes Complicit: Mayors, Criminal Actors, and the Deliberate Weakening of the Local State in Colombia". In: *Comparative Political Studies*, p. 00104140221139380.

NPR Fresh Air (2021). "Inner Workings Of DarkSide Cybergang Reveal It's Run Like Any Other Business". In: URL: https://www.npr.org/2021/06/10/1005093802/inner-workings-of-darkside-cybergang-reveal-its-run-like-any-other-business.

OECD (2023). *Enterprises by business size (indicator)*. https://data.oecd.org/entrepreneur/enterprises-by-business-size.htm. Accessed on June 2, 2023.

Ottis, Rain (2008). "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective". In: *Proceedings of the 7th European Conference on Information Warfare*. Academic Publishing Limited Reading, MA, p. 163.

Page, Carly (2023). "Police arrest suspected members of prolific DoppelPaymer ransomware gang". In: URL: https://techcrunch.com/2023/03/06/police-arrest-suspected-members-of-prolific-doppelpaymer-ransomware-gang/.

Palmer, Danny (2021). "Ransomware: Russia told to tackle cyber criminals operating from within its borders". In: URL: https://www.zdnet.com/article/ransomware-russia-told-to-tackle-cyber-criminals-operating-from-within-its-borders/.

Perlroth, Nicole and David E. Sanger (2022). "Ransomware Attacks Take On New Urgency Ahead of Vote". In: *The New York Times*. URL: https://www.nytimes.com/2020/10/12/us/politics/election-hacking-microsoft.html.

Podlosky, Adam and Brendon Feeley (2021). "Indrik Spider Supersedes WastedLocker with Hades Ransomware to Circumvent OFAC Sanctions". In: URL: https://www.crowdstrike.com/blog/hades-ransomware-successor-to-indrik-spiders-wastedlocker/.

Price, Ned (2022). "Reward Offers for Information to Bring Conti Ransomware Variant Co-Conspirators to Justice". In: URL: https://www.state.gov/reward-offers-for-information-to-bring-conti-ransomware-variant-co-conspirators-to-justice/.

Profero (2021). "Cuba Ransomware Group on a Roll". In: URL: https://profero.io/posts/cubaransomware/Cuba-Ransomware-Group-on-a-roll.pdf.

Puhr, Rainer et al. (2017). "Firth's logistic regression with rare events: accurate effect estimates and predictions?" In: *Statistics in medicine* 36.14, pp. 2302–2317.

Rising, David (2023). "Report: Chinese state-sponsored hacking group highly active". In: *AP News*. URL: https://apnews.com/article/china-hacking-report-redgolf-insikt-88a76977ce50d6d28d7a1be5130a1aa7.

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.

Shakarian, Paulo (2011). "The 2008 Russian cyber campaign against Georgia". In: *Military Review-English Edition* 91.6, p. 63.

Siniawer, Eiko Maruko (2012). "Befitting bedfellows: Yakuza and the state in modern Japan". In: *Journal of Social History* 45.3, pp. 623–641.

Skarbek, David (2011). "Governance and prison gangs". In: *American Political Science Review* 105.4, pp. 702–716.

— (2016). "Covenants without the sword? Comparing prison self-governance globally". In: *American Political Science Review* 110.4, pp. 845–862.

Stone-Gross, Brett, Sergei Frankoff, and Bex Hartley (2019). "BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0". In: URL: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/.

Stubbs, Jack (2017). "Russian hacker wanted by U.S. tells court he worked for Putin's party". In: URL: https://www.reuters.com/article/us-usa-cyber-botnet/russian-hacker-wanted-by-u-s-tells-court-he-worked-for-putins-party-idUSKCN1C32EP.

The White House (2022). *Statement by President Biden on our Nation's Cybersecurity*. https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/statement-by-president-biden-on-our-nations-cybersecurity/.

The World Bank (2021). *World Development Indicators 2012: GDP per capita, Atlas method*. Data file. URL: https://databank.worldbank.org/reports.aspx?source=world-development-indicators.

Tilly, Charles (1985). "War Making and State Making as Organized Crime". In: *Violence: A Reader*. Ed. by Catherine Besteman. Washington Square, New York, USA: New York University Press. Chap. 4, pp. 35–60.

Toulas, Bill (2021). "PYSA ransomware behind most double extortion attacks in November". In: URL: https://www.bleepingcomputer.com/news/security/pysa-ransomware-behind-most-double-extortion-attacks-in-november/.

— (2022a). "Clop ransomware uses TrueBot malware for access to networks". In: URL: https://www.bleepingcomputer.com/news/security/clop-ransomware-uses-truebot-malware-for-access-to-networks/.

— (2022b). "Cuba ransomware affiliate targets Ukrainian govt agencies". In: URL: https://www.bleepingcomputer.com/news/security/cuba-ransomware-affiliate-targets-ukrainian-govt-agencies/.

Trejo, Guillermo and Sandra Ley (2018). "Why did drug cartels go to war in Mexico? Subnational party alternation, the breakdown of criminal protection, and the onset of large-scale violence". In: *Comparative Political Studies* 51.7, pp. 900–937.

— (2021). "High-profile criminal violence: Why drug cartels murder government officials and party candidates in Mexico". In: *British Journal of Political Science* 51.1, pp. 203–229.

Trend Micro Research (2022a). "Ransomware Spotlight: Clop". In: URL: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-clop.

— (2022b). "Ransomware Spotlight: Cuba". In: URL: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-cuba.

Tunney, Catharine (2023). "Intelligence agency says ransomware group with Russian ties poses 'an enduring threat' to Canada". In: URL: https://www.cbc.ca/news/politics/cse-lockbit-threat-1.6734996.

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

U.S. Department of Justice (2020). "State-Sponsored Iranian Hackers Indicted for Computer Intrusions at U.S. Satellite Companies". In: URL: https://www.justice.gov/opa/pr/state-sponsored-iranian-hackers-indicted-computer-intrusions-us-satellite-companies.

— (2021). "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe". In: URL: https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

— (2022). "Russian and Canadian National Charged for Participation in Lockbit Global Ransomware Campaign". In: URL: https://www.justice.gov/usao-nj/pr/russian-and-canadian-national-charged-participation-lockbit-global-ransomware-campaign.

U.S. Department of the Treasury (2019). "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware". In: URL: https://home.treasury.gov/news/press-releases/sm845.

Valeriano, Brandon, Benjamin M Jensen, and Ryan C Maness (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

Varese, Federico (2018). *Mafia life: Love, death, and money at the heart of organized crime*. Oxford University Press.

Villadsen, Ole, Charlotte Hammond, and Kat Weinberger (2022). "Unprecedented Shift: The Trickbot Group is Systematically Attacking Ukraine". In: URL: https://securityintelligence.com/posts/trickbot-group-systematically-attacking-ukraine/.

Wing, Coady (2021). "Statistical Inference For Stacked Difference in Differences and Stacked Event Studies". In: Indiana University Workshop in Methods.

Yale School of Management (n.d.). *Over 1,000 Companies Have Curtailed Operations in Russia, but Some Remain*.

Appendices

A Group Classification

Below, we provide a brief description of our rationale for classifying seven groups as Russia based. We also provide a brief description for three other groups that are known to have Russian speaking members, yet we have not classified as Russia-based groups because we have not found evidence linking the groups to Russia.

A.1 Groups with Russian Ties

Below are a list of groups that we have classified as Russia-based in our analysis, which we have classified as such because cybersecurity researchers have identified these groups as having core members operating from within Russia. Some groups may have members that also operate from other countries.

A.1.1 CL0P

CL0P ransomware is a successor of CryptoMix ransomware, which was developed in Russia and used by groups such as FIN11, a financially motivated Russian cybercriminal group (Health Sector Cybersecurity Coordination Center 2023; Toulas 2022a). CL0P is operated by a Russian-speaking group (Trend Micro Research 2022a) that showed a decrease in activity during the Russian New Year and Orthodox Christmas holidays (Ilascu 2020). CL0P ransomware also avoids executing on computers with a Commonwealth of Independent States language language keyboard installed (Ilascu 2020). The Commonwealth of Independent States is a regional intergovernmental organization made up of former Soviet states.

Most tellingly, the group's activity persisted following the arrest of operatives in Ukraine, and security experts confirmed that they believe the group's key personnel are based in Russia. Cybersecurity company Intel 471 stated, "The law enforcement raids in Ukraine

associated with CLOP ransomware were limited to the cash-out/money laundering side of CLOP's business only" (Gatlan 2021). Intel 471 then confirmed that they believe the group's core actors operate from Russia (Krebs 2021). Soon after these arrests, CL0P resumed its ransomware operations.

A.1.2 Conti

The strain of ransomware used by the Conti group was developed by the cybercriminal group Wizard Spider, which has pledged its support for the Russian government (CISA, NSA, FBI, ACSC, CCCS, NZ NCSC, NCSC-UK, and the UK National Crime Agency (NCA) 2022, p. 10). Members of the Conti ransomware group were based in Russia, and the group's leaders maintained ties with the FSB (Bing 2022; Podlosky and Feeley 2021).

A.1.3 Cuba

Security researchers believe the Cuba ransomware gang operates out of Russia because the Cuba ransomware strain avoids infecting computers with a Russian keyboard installed (Trend Micro Research 2022b). Other researchers have determined that group members speaks Russian (Profero 2021, pp. 9–10) and use malware that originates from Russian groups (Hope 2021). In October 2022, Cuba ransomware was used to target Ukrainian government agencies (Toulas 2022b).

A.1.4 DarkSide

In 2020, Carbon Spider (also known as FIN17) established DarkSide as a Ransomware as a Service (RaaS) division of REvil ransomware (Loui and Reynolds 2021). The group communicates in Russian and appears to operate from within Russia (NPR Fresh Air 2021). The group's ransomware did not target victims in the Commonwealth of Independent States (Kramer, Schwirtz, and Troianovski 2021).

A.1.5 DoppelPaymer

DoppelPaymer is a rebranding of BitPaymer ransomware, which is a ransomware strain developed by Russia-based cybercriminal group Indrik Spider (Stone-Gross, Frankoff, and Hartley 2019; Podlosky and Feeley 2021). However, DoppelPaymer's code includes important differences from BitPaymer's code, which suggests that one or more members of Indrik Spider may have broken away to form the DoppelPaymer ransomware group (Stone-Gross, Frankoff, and Hartley 2019). Given this group's origins from Indrik Spider, we classify DoppelPaymer as a Russia-based group.

A.1.6 Grief

Grief is tied to Evil Group, a Russian cybercriminal group that was sanctioned by the U.S. government (Abrams 2021). Grief is also believed to be a rebranding of the previous ransomware group DoppelPaymer (Ilascu 2021).

A.1.7 Sodinokibi (REvil)

Evil Corp, the group behind REvil, was identified as a Russia-based cybercriminal group and sanctioned by the U.S. Treasury Department's Office of Foreign Assets Control in December 2021 (U.S. Department of the Treasury 2019).

A.2 Other Groups

Below are several groups known to have Russian speaking members, but reliable cybersecurity researchers have not attributed the group's operations to Russia. This distinction is important, because we wish to distinguish groups that operate largely from within Russia from those that are merely part of the broader Eastern European cybercriminal ecosystem. Accordingly, we *do not* classify these groups as Russia-based groups.

A.2.1 Egregor

In February 2021, Ukrainian officials arrested members of the Egregor ransomware gang; by the time of the arrest, the group had become largely defunct (Cimpanu 2021b).

A.2.2 Everest

Everest is a Russian-speaking ransomware group (Toulas 2021). However, there is no further evidence that core members operate from Russia.

A.2.3 LockBit

Security researchers have documented that members of LockBit communicate in Russian but have stopped short of stating that the group likely operates out of Russia (Field 2023; Tunney 2023). In November 2022, U.S. attorneys arrested and charged a Canadian and Russian citizen for his involvement with LockBit (U.S. Department of Justice 2022).

A.3 List of Groups in Dataset

Table 6: Ransomware Group Statistics

Group	Number of Victims	First Attack	Last Attack	Russia-Based	Commonwealth of Independent StatesAvoiding[†]
AKO	9	05-13-20	07-08-20		
Alpha VM	42	01-07-22	03-08-22		
Arvin Club	11	11-09-21	04-26-22		
Astro Team	15	02-03-21	04-22-21		
Avaddon	181	08-20-20	06-09-21		✔
Avos Locker	55	07-08-21	04-04-22		
Babuk 2.0	4	06-15-21	07-27-21		
BABUK LOCKER	43	01-03-21	05-14-21		✔
BlackByte	12	09-13-21	09-13-21		
Bonaci	3	11-30-21	11-30-21		
CL0P	118	08-20-20	06-22-21	✔	✔
Conti	842	01-09-20	06-03-22	✔	✔
Cuba	12	11-15-20	06-25-21	✔	
DarkSide	99	08-08-20	05-13-21	✔	✔
DoppelPaymer	203	02-21-20	05-06-21	✔	✔
Egregor	204	09-25-20	12-30-21		
Entropy	9	–	–		
Everest	65	12-02-20	06-25-21		
Grief	85	05-27-21	01-10-22	✔	
Haron	1	07-17-21	07-17-21		
Hive	109	06-24-21	05-22-22		
Lockbit	494	09-17-20	05-10-22		
LOCKDATA	7	06-08-21	06-08-21		
Lorenz	33	12-20-20	04-19-22		
LV	75	03-07-21	02-18-22		

B Victim Size

We compare the size of victims targeted by Russia-based and other groups as the size of a group's victims reveals important information about its capabilities. Specifically, size is important because only groups with greater capabilities can attack larger companies,[18] and accordingly, we focus on two common indicators of size – a company's total assets and number of employees. We hypothesize that *if* Russia-based groups receive resources from the government, this could allow them to develop greater capabilities and target larger victims on average. However, there are several reasons the Russian government might be reluctant to provide resources to ransomware groups *even if* they maintain a cooperative relationship, including the fear that a group with increased power could turn its strength against the state (Borghard and Lonergan 2016).

B.1 Data

To enable this analysis, we matched our dataset of ransomware victims with company data provided by the Orbis global database from Bureau van Dijk, which is the largest cross-country firm-level database and includes financial information from both public and private companies (Kalemli-Ozcan et al. 2015). We construct additional matches using the Compustat North America by Standard & Poor's and Worldscope by Thomson Financial datasets. We identify matches across these datasets using a victim's website address or a victim's name, address, and sector. We obtain 1,309 matches our 4,194 total victims, including 375 small businesses, 287 medium-size businesses, and 430 large businesses based on the OECD's classification system, which uses a company's number of employees (OECD 2023).[19] Because financial datasets typically have better coverage of large companies, we expect that unmatched victims are more likely to be small companies (Kalemli-Ozcan et al. 2015).

[18] Examples of greater capabilities include conducting reconnaissance before an attack over a longer period of time or engaging in sophisticated social engineering schemes (Cybereason 2022, pp. 2–3).

[19] Two hundred and seventeen companies lacked data on the number of employees.

Table 1: Ransomware Group Statistics (Continued)

Group	Number of Victims	First Attack	Last Attack	Russia-Based	Commonwealth of Independent StatesAvoiding†
Marketo	40	04-13-21	07-20-21		
MAZE	262	12-07-19	11-05-20		
Midas	32	–	–		
Mount Locker	20	09-22-20	03-29-21		✔
N3tw0rm	4	05-02-21	05-19-21		
Nefilim	41	03-20-20	07-20-21		✔
NEMTY	1	03-03-20	03-03-20		
NetWalker	144	01-11-20	01-26-21	✔	✔
Pay2Key	9	11-04-20	12-28-20		
Payload.bin	25	05-31-21	10-19-21		
Prometheus	48	03-27-21	07-13-21		
Pysa	270	01-12-20	12-02-21		✔
Quantum	16	07-15-21	02-28-22		
Ragnar Locker	41	06-11-20	02-28-22		✔
Ragnarok	33	12-23-20	04-09-21		✔
RansomEXX	37	11-30-20	12-15-21		✔
Ranzy Locker	3	10-16-20	11-06-20		
Sekhmet	6	03-23-20	06-29-20		
Snatch	37	11-21-21	12-10-22		
Sodinokibi (REvil)	281	05-13-20	07-10-21	✔	✔
Suncrypt	34	08-01-20	02-28-21		
SynACK	7	03-28-21	06-16-21		
Team Snatch	6	05-01-19	05-17-19		
Vice Society	29	05-25-21	07-17-21		
Xing Locker	24	04-29-21	10-26-21		

Notes: This table shows all ransomware groups in in the dataset along with their total number of victims, the dates of their first and last attacks, whether we have classified the group as Russia-based, and whether the group's ransomware avoids Commonwealth of Independent Statescountries. † Malwarebytes Labs (2021) identifies Commonwealth of Independent Statesavoiding malware.

Table 7: Descriptive Statistics for Russia-Based and Other Groups

Variable		Min	Max	Mean	Median	SD	*N*
Total assets (B USD)							
	Other Groups	0	878.9	2.7	0.02	33.1	741
	Russia-Based Groups	0	569.5	3.8	0.04	33.5	568
Total employees							
	Other Groups	1	540,667	4,850	105	27,497	602
	Russia-Based Groups	1	668,856	4,394	168	33,853	490

Notes: Descriptive statistics include the minimum, maximum, mean, median, standard deviation and count (N) of victims' total assets (in billions of dollars) and victims' total employees for all victims attacked by Russia-based and other groups.

B.2 Estimation

We estimate the relationship between Russia-based groups and victim size with the following model:

$$\text{Victim Size}_i = \alpha + \beta\text{Russia-based Group} + \delta\text{Time} + \gamma_k + \theta_m + \epsilon_{ikm}, \tag{4}$$

where k is the victim's sector and m is the victim's country. *Russia-based Group* is a binary variable indicating whether the group behind the attack is linked to Russia. This approach allows us to model covariates that correlate with the size of a victim: when an attack took place and a victim's country and sector. We estimate the model twice, once with size measured by total assets and once measured by the number of employees (taking the log of both outcomes).

Table 8 shows that *we do not* find a statistically significant relationship between Russia-based groups and the size of a victim for either the baseline models or models with additional covariates included. To test the robustness of these findings, we measure the relationship between victim size and Russia-based groups using an alternate specification of company size: a categorical variable denoting small, medium, and large companies based on the OECD's classification system (OECD 2023). Table 9 shows that once again, we do not find a statistically significant relationship between victim size and Russia-based groups (Appendix **??**).

Table 8: Victim Size and Russia-Based Groups

	Total Assets (Log)		Total Employees (Log)	
	(1)	(2)	(3)	(4)
Russia-Based Group	0.319	0.279	0.285	0.276
	(0.200)	(0.208)	(0.149)	(0.157)
Constant	17.018***	13.861***	5.030***	3.090**
	(0.132)	(3.440)	(0.100)	(1.149)
Month-year (Linear)		✓		✓
Sector FEs		✓		✓
Country FEs		✓		✓
Observations	1,309	1,199	1,092	1,006
R^2	0.002	0.189	0.003	0.170
Adjusted R^2	0.001	0.125	0.002	0.104

Notes: Table shows the relationship between group type and the total assets (logged) and number of employees (logged). Data includes attacks between June 1, 2018 and April 30, 2022. Standard errors are in parentheses; stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

Thus, our findings show that Russia-based groups *do not* target larger victims on average, which suggests that they do not have greater capabilities on average than other groups; in turn, this suggests that Russia *does not* provide resources to ransomware groups that significantly enhances their capabilities.

Table 9: Victim Size (Categorical) and Russia-Based Groups

	Company Size (small, medium, large)			
	(1)	(2)	(3)	(4)
Russian	0.056	0.046	0.038	0.069
	(0.040)	(0.041)	(0.040)	(0.042)
Constant	1.571***	1.734***	1.611***	1.148***
	(0.027)	(0.063)	(0.107)	(0.167)
Month-Year (Linear)	✓			✓
Sector FEs		✓		✓
Country FEs			✓	✓
Observations	1,309	1,258	1,281	1,199
R^2	0.001	0.007	0.047	0.206
Adjusted R^2	0.001	0.005	0.037	0.144

Notes: Robust standard errors are in parentheses; stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

C Victims by Sector

Table 11 shows the relationship between the proportion of victims by sector for Russia-based and other groups. Russia-based groups carry out a *greater* proportion of attacks against victims in the consumer discretionary sector and a *smaller* proportion of attacks against victims in the education and communication services; these results are statistically significant based on a chi-squared test. Over all, results by sector do not point to a major difference in the targeting strategies of Russia-based and other groups, as both tend to target

Table 10: 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

a relatively similar proportion of victims from each sector. Thus, while there are notable differences in the targeting of victims by country for Russia-based and other groups, the differences in terms of sector are limited.

Table 11: Victims by Sector

	Other Groups		Russia-Based		χ^2	p-value
	N	(%)	N	(%)		
Industrials	603	26.3	481	28.0	1.394	0.238
Consumer Discretionary	328	14.3	293	17.1	5.524	0.019
Other Services	206	9.0	155	9.0	0.0	1.0
Information Technology	173	7.5	117	6.8	0.672	0.413
Materials	172	7.5	133	7.7	0.054	0.817
Health Care	153	6.7	98	5.7	1.392	0.238
Financials	137	6.0	91	5.3	0.709	0.400
Education	108	4.7	42	2.4	13.34	0.000
Consumer Staples	101	4.4	95	5.5	2.457	0.117
Public Administration	99	4.3	63	3.7	0.900	0.343
Communication Services	76	3.3	38	2.2	3.916	0.048
Real Estate	57	2.5	44	2.6	0.003	0.958
Energy	43	1.9	36	2.1	0.149	0.700
Utilities	39	1.7	32	1.9	0.071	0.789
Total	2,295		1,713			

Notes: Table shows the number of victims by sector for Russia-based and other groups. Each χ^2 value relates to the null hypothesis that there is no difference in the proportion of victims in each sector for both types of groups.

Table 12: Daily Attacks by Russia-Based and Other Groups

	Russia-Based Groups	Other Groups
	(1)	(2)
Time_{-3}	0.511	0.018
	(0.341)	(0.149)
Time_{-2}	0.381^{**}	0.198
	(0.125)	(0.212)
Time_{-1}	0.308^{**}	0.036
	(0.117)	(0.218)
Time_{0}	0.044	0.374
	(0.112)	(0.284)
Time_{+1}	0.051	0.127
	(0.111)	(0.115)
Time_{+2}	-0.081	-0.019
	(0.101)	(0.094)
Time_{+3}	0.105	-0.114
	(0.107)	(0.077)
Germany	-1.192^{***}	-0.566^{*}
	(0.225)	(0.228)
UK	-0.094^{***}	-0.042^{*}
	(0.023)	(0.021)
USA	0.991^{***}	1.127^{***}
	(0.159)	(0.202)
Time (*Linear*)	0.057^{***}	0.029^{**}
	(0.010)	(0.010)
Constant	-0.517^{***}	-0.238^{**}
	(0.071)	(0.087)
Observations	1,444	1,444
R^2	0.197	0.165
Adjusted R^2	0.191	0.159

Notes: Robust standard errors are in parentheses; stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

D Main Results: Attacks by Russia-Based and Other Groups

D.1 Full Model

D.2 Robustness Check

As a robustness check, we estimate Equation 1 with an alternate binary specification of the dependent variable that is coded as one if there is at least one ransomware attack on a given day and zero otherwise. Once again, we estimate the model twice – once for the number of attacks by Russia-based groups and once for the number of attacks by other groups. The results of this analysis are presented in Table 13. Similar to our findings with the main specification, there is a positive and statistically significant increase in the number of attacks by Russia-based groups during the three, two, and one months before the election period with no similar increase in attacks by other groups.

D.3 Attacks by Russia-Based Groups by Sector

Figure 4 shows coefficient plots for the number of daily attacks in the periods close to elections by Russia-based groups disaggregated by sector. We estimate the following model:

$$\text{At Least One Attack}_{jd} = \beta_0 + \beta_1 \text{Time to Election}_j + \beta_2 \text{Time} + \gamma_j + \epsilon_{jmd}, \tag{5}$$

where j is the country, *Time* is a linear time trend capturing the month and year, and the outcome is a binary variable indicating whether there was at least one attack against a victim in that sector on a given day. We use the `logistf` package in `R`, which provides corrections for the bias introduced by the dependent variables' small number of events (i.e., days with at least one attack for each sector). Using the package, we fit a logistic regression model

Table 13: Days with At Least One Attack by Russia-Based Groups

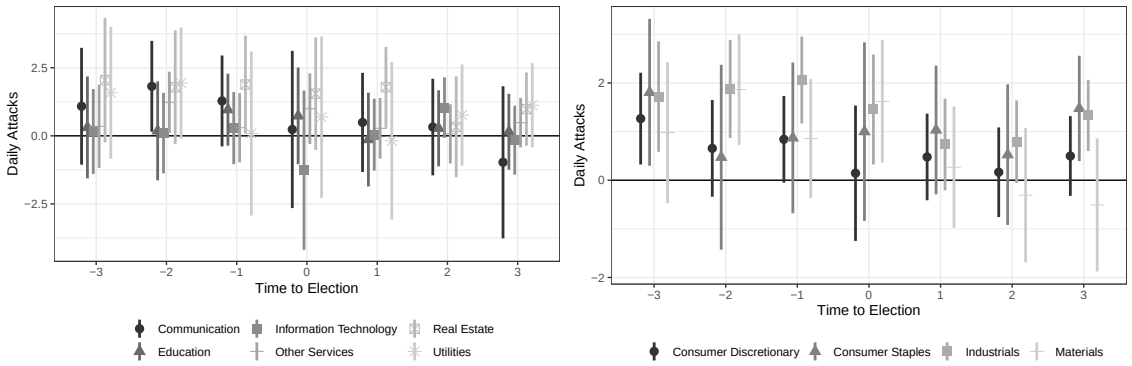
	Russia-Based Groups	Other Groups
	(1)	(2)
Time_{-3}	0.078^{**}	-0.036
	(0.030)	(0.027)
Time_{-2}	0.088^{**}	0.013
	(0.029)	(0.027)
Time_{-1}	0.073^{**}	0.002
	(0.026)	(0.030)
Time_{0}	0.041	0.042
	(0.039)	(0.042)
Time_{+1}	0.042	0.054
	(0.028)	(0.031)
Time_{+2}	0.019	0.002
	(0.033)	(0.030)
Time_{+3}	0.062^{*}	0.067
	(0.031)	(0.036)
Germany	-0.238^{***}	-0.137^{*}
	(0.060)	(0.062)
UK	-0.024^{***}	-0.009
	(0.006)	(0.009)
USA	0.364^{***}	0.390^{***}
	(0.039)	(0.041)
Time (*Linear*)	0.016^{***}	0.010^{***}
	(0.002)	(0.003)
Constant	-0.143^{***}	-0.076^{***}
	(0.020)	(0.020)
Observations	1,444	1,444
R^2	0.394	0.344
Adjusted R^2	0.389	0.339

Notes: Robust standard errors are in parentheses; stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

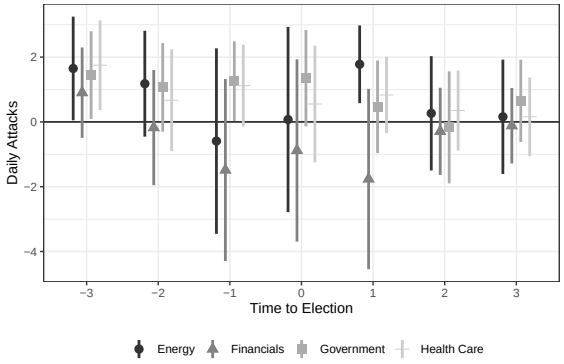
Figure 4: Attacks by Russia-Based Groups by Sector

(a) Services

(b) Materials and Finished Goods



(c) Essential Services



Notes: Figures show coefficient plots, including point estimates and confidence intervals, for the effect of time to election on the number of ransomware attacks by Russia-based groups across sectors. Each model is estimated separately.

with Firth's bias reduction method for rare events (Puhr et al. 2017).

E Analysis Using Chainalysis Data

We use data from Chainalysis to assess whether there is an increase in payments to Russia-based ransomware groups before elections. We estimate the following model:

$$\text{Payments to Ransomware Groups}_d = \beta_0 + \beta_1 \text{Time to Election} + \beta_2 \text{Time}_m + \epsilon_{md}, \qquad (6)$$

where *Payments to Ransomware Groups* denotes the number of payments to ransomware groups on a given day, *Time to Election* indicates whether a given day is close to an election, and *Time* is a month-year linear trend. We estimate this model for the twelve months surrounding three U.S. elections: the 2016 and 2020 presidential elections and the 2018 U.S. midterm elections.

Table 14 shows the results of our analysis. Similar to our analysis based on the number of attacks before elections, we find an increase in the number of payments to ransomware groups two months before election periods with no similar increase in the number of payments to other groups. We also find a positive and statistically significant increase in the number of ransomware payments to Russia-based groups two months before elections for the more conservative sample that includes only the number of payments before the 2016 and 2018 elections.

F Alternate Explanations for Post-Invasion Decrease in Ransomware Attacks

There are two alternate explanations for the decrease in ransomware attacks after the invasion, but we argue that neither adequately explains the decrease in attacks. One alternate explanation is that the Russian government constrained ransomware groups prior to the invasion to minimize the risk of inadvertent crisis escalation; indeed, the Kremlin arrested nearly a dozen members of a ransomware group one month before the invasion (Nechepurenko 2022). However, we argue that these arrests were more likely aimed at creating diplomatic leverage over foreign actors rather than constraining activity from ransomware groups, as they targeted a well known group that was no longer in operation rather than one of the many groups still actively carrying out attacks (Collier 2022).

A second explanation is that ransomware groups and their activities were disrupted by increased cooperation from Western governments and companies. Although Western

Table 14: Effect of Elections on Payments to Ransomware Groups

	Number of Ransomware Payments	
	Russia-based	Other Groups
	(1)	(2)
Time_{-3}	0.204	-15.278^{***}
	(0.146)	(2.859)
Time_{-2}	0.509^{**}	-6.496
	(0.157)	(3.423)
Time_{-1}	0.058	-12.777^{***}
	(0.120)	(2.825)
Time_{0}	0.083	-19.756^{***}
	(0.242)	(3.427)
Time_{+1}	-0.166	-11.150^{***}
	(0.116)	(2.913)
Time_{+2}	-0.305^{**}	-12.115^{***}
	(0.108)	(2.575)
Time_{+3}	-0.333^{***}	3.852
	(0.095)	(4.228)
Time (*Linear*)	0.040^{***}	-2.311^{***}
	(0.004)	(0.117)
Constant	-0.143^{*}	90.764^{***}
	(0.062)	(3.526)
Observations	1,080	1,080
R^2	0.134	0.379
Adjusted R^2	0.127	0.375

Notes: Robust standard errors are in parentheses; stars denotes statistical significance levels at *p<0.05; **p<0.01; ***p<0.001

governments and cybersecurity companies increased information sharing and cooperation after the invasion, it is unlikely to have had a major impact on ransomware activity as these actors have primarily focused on disrupting other types of cyber attacks directed against Ukraine (Google 2023). Thus, we argue that the decrease in cyber attacks following the invasion is most likely driven by the Russian government's recruitment of ransomware operators to aid its cyber offensive against Ukraine.

G Attacks Against Specific Companies

G.1 Full Model

G.2 Robustness Check

To test the robustness of our findings in Section 4.3, we estiamate the following model:

$$\begin{aligned}\text{Attacks Against A or B Rated Companies}_{jmti} = \beta_0 + \beta_1 \text{Invasion}_i + \beta_2 \text{Time}_t + \gamma_j \\ + \delta_m + \epsilon_{jtmi},\end{aligned} \tag{7}$$

where j is a country in which a victim is located, m is the month, and t is the month-year. The outcome variable is coded as one if an attack is against an A or B rated company and zero others (an attack against another company). *Invasion* is a dummy variable indicating the post-invasion period. We are primarily interested in β_1, which is the effect of being in the post-invasion period on the likelihood of an attack against an A or B rated company. We also include a month-year linear time trend (β_2) and fixed effects for a victim's country (γ) and the month of the attack (δ).

Table 16 shows that there is a positive and statistically significant relationship between the number of attacks against A or B rated companies and the post-invasion period, which corresponds with a roughly two percent greater chance that a victim targeted in the post-invasion period is an A or B rated company. This means that A or B rated companies

Table 15: Number of Daily Attacks for A or B Rated Companies Post Invasion

	Number of Daily Attacks
Post Invasion	-3.265^{***}
	(0.705)
A/B Rated Companies	-5.498^{***}
	(0.242)
Month-year	-0.007
	(0.021)
Month_2	1.514^{***}
	(0.577)
Month_3	1.878^{***}
	(0.624)
Month_4	1.905^{***}
	(0.626)
Month_5	0.670
	(0.585)
Month_6	0.659
	(0.584)
Month_7	-0.259
	(0.574)
Month_8	0.844
	(0.570)
Month_9	1.397^{**}
	(0.571)
Month_10	1.165^{**}
	(0.564)
Month_11	2.261^{***}
	(0.566)
Month_12	1.364^{**}
	(0.561)
Post Invasion × A/B Rated Companies	2.559^{***}
	(0.805)
Constant	4.595^{***}
	(0.522)
Observations	1,460
R^2	0.285
Adjusted R^2	0.278
Note:	*p<0.1; **p<0.05; ***p<0.01

Table 16: Attacks Against A or B Rated Companies Post Invasion

	Attacks Against A or B Rated Companies			
	(1)	(2)	(3)	(4)
Post Invasion	0.017*	0.019**	0.023**	0.019*
	(0.007)	(0.007)	(0.008)	(0.009)
Constant	0.009***	0.000	0.007	0.008
	(0.002)	(0.057)	(0.057)	(0.058)
Country FEs		✓	✓	✓
Month FEs				✓
Month-Year (Linear)			✓	✓
Observations	4,032	3,831	3,831	3,831
R^2	0.002	0.033	0.033	0.035
Adjusted R^2	0.001	0.007	0.008	0.006

Notes: Table shows that there is a positive and statistically significant relationship between the number of attacks against A or B rated companies (or their subsidiaries) and post-invasion period. Standard errors are in parentheses. Data on company ratings provided by the Yale CELI list. The number of observations decreases between models 1 and 2 because we were unable to locate the country of some victims. Stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.

were more likely to experience a ransomware attack after the invasion than before (although the overall rate of attack remains low); this finding is robust to the inclusion of time trend variables and country fixed effects.

Table 17 shows the relationship between the number of attacks against C-F rated companies (according to the Yale CELI List of Companies) and the post-invasion period. The results show that there is no statistically significant difference in the likelihood that C-F rated companies will be targeted with attacks following the invasion. See Section 4.3 for more details.

Table 17: Attacks Against C-F Rated Companies Post Invasion

	Attacks Against C-F Rated Compaies			
	(1)	(2)	(3)	(4)
Post Invasion	−0.002	−0.004	−0.001	−0.001
	(0.005)	(0.006)	(0.006)	(0.007)
Constant	0.006***	−0.000	0.004	0.006
	(0.001)	(0.046)	(0.046)	(0.046)
Country FEs		✓	✓	✓
Month FEs				✓
Month-Year (Linear)			✓	✓
Observations	4,032	3,831	3,831	3,831
R^2	0.00003	0.021	0.022	0.024
Adjusted R^2	−0.0002	−0.004	−0.004	−0.004

Notes: Table shows the number of attacks against C-F rated companies based on the Yale CELI List of Companies categorizing companies' responses to Russia's invasion of Ukraine. Standard errors are in parentheses and stars indicate the statistical significance level: *p<0.05; **p<0.01; ***p<0.001.