ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

The State in Ransomware: Evidence of Concentration and Targeting Patterns among Russian-Affiliated Groups

Aaron Brantly | Tech for Humanity Lab and the School of Public and International Affairs, Virginia Tech, USA | ORCID: 0000-0003-4193-3985

Ryan Mason | Tech for Humanity Lab, Virginia Tech, USA| ORCID: 0009-0005-8946-7604

Abstract

Ransomware is increasingly associated with states that seek to undermine adversaries. This work builds a theoretical argument through case studies and an open-source database of 19,128 instances of ransomware attacks that quantitatively and qualitatively identifies patterns consistent with a permissive environment within the Russian Federation for ransomware activities that target the economic and political interests of its perceived adversaries during a time of war. These ransomware attacks facilitate indirect revenues through taxation to the Russian economy and direct revenues to Russian criminal entities, undermine the economies and industries of adversaries, and occur within a Russian information environment that is highly constrained and insular. The central question of this work examines whether criminal ransomware group activities align with state interests. Russian ransomware activities likely complement other attributes of Russia's information warfare and propaganda strategy leading to an increasingly contested digital environment. By using data-driven analysis, this work builds on prior case analyses and establishes with quantitative evidence in the form of leak-site data that while ransomware is often considered a global cybercrime problem, the volume and

Received: 17.12.2025

Accepted: 23.02.2026

Published: 05.03.2026

Cite this article as:
A. Brantly, R. Mason, "The state in ransomware: Evidence of concentration and targeting patterns among Russian-affiliated groups," ACIG, vol. 5, no. 1, 2026, doi: 10.60097/ACIG/219041.

Corresponding author:
Aaron Brantly, Tech for Humanity Lab in the School of Public and International Affairs, Virginia Tech, USA; E-mail: abrantly@vt.edu
0000-0003-4193-3985

directionality of ransomware attacks indicate that a disproportionate share of ransomware within our dataset has Russian origins.

Keywords
Russia, ransomware, war

1. Introduction

The global distribution of ransomware attacks increasingly indicates a pattern of behaviour suggestive of state cooptation or state condoning of criminal activities targeted against perceived adversaries. This analysis uses an open-source database of 19,128 cases of ransomware attacks against different entities to demonstrate the disproportionate use of ransomware originating within the Russian Federation or Russian-affiliated groups. Our data includes information on attacks and lifespan of more than 110 ransomware groups over a period of 2 years. We present both the data on and the logic for the state use, cooptation, or condoning of criminal ransomware activities to further the interests of the host state. Disruptions of critical infrastructure, including power systems, hospitals, educational institutions, or industry, are all increasingly commonplace. Tactics ranging from standalone ransomware to ransomware as a service have varying levels of impact and financial reward. By undermining confidence in networks, and systems, the attacks increase costs and drive a cycle of insecurity within targeted states, bring direct and indirect financial rewards resulting from ransom payments and potential taxes on those payments or on the salaries of the employees of ransomware gangs. The result is a criminal–state nexus that violates international and national laws.

This paper builds the argument that global ransomware arises due in large part to lack of due diligence by the Russian Federation to police its own digital spaces. Russia's apparent inability to control ransomware groups originating within its borders is consistent with selective enforcement/under enforcement as will be demonstrated through an analysis of its control of domestic internet networks. Moreover, the use of ransomware seems to be directionally oriented towards eroding public trust in digital networks and systems in non-aligned states. While at times ransomware attacks are targeted to achieve maximum effect, overwhelmingly these attacks are designed to foster chaos and undermine the security of perceived adversarial nations. The secondary benefits of the ransomware market are in line with other state-based ransomware

actors and primarily revolve around an influx of illicitly gained capital resulting from ransom payments, intellectual property, trade secrets, and other geoeconomic and geostrategic advantages that arise.

All analyses of Russian involvement in its prolific ransomware industry are based largely on circumstantial evidence. Yet by combining multiple types of circumstantial evidence, our research supports and builds upon the cases developed by other scholars who have identified a state–criminal nexus that is having a profound impact on global cybersecurity. This evidence is built through the theoretical frameworks of state–criminal network cooptation, informal and formal direction, and collaboration between criminal and state enterprises. These actions extend the literature typically focused on the mafia state and highlight the geopolitical and geostrategic impact of state–criminal interactions within Russian cyberspace and beyond. In addition to theorising the relationship and providing micro-case examples from ransomware activities over the last 10 years, we also demonstrate that the Russian state fails to adhere to internationally recognised principles of due diligence over its domestic Internet within the area of cybercrime. Finally, we use data to demonstrate that the ransomware problem faced by most countries is not a global cybercrime problem but predominantly cybercrime problem of Russian origin.

2. Mafia State, Privateers, Geopolitics, and Convenience

Russia's relationship to its cyber criminals is complex and parallels its wider relationship with its other criminal elements. In many ways, Russia has established a unique relationship with its criminal elements built on convenience, corruption, and state power. Some authors contend that Russia is a mafia state. A state in which the government, government officials, police, and military become deeply interwoven with organised criminal elements. McCarthy-Jones and Turner provide an extensive analysis of the structural frameworks of different types of mafia states and raise concerns that the basic definition of connections between members of a state's government and criminal networks oversimplifies and thereby does not adequately address the nuance and complexity of different types of mafia states and how they are formed [1]. They note that the term mafia state has been applied to at least 20 different countries and that the application of this term varies from state to state [1]. What they do note is that among all 'mafia' states and within the broader literature, there are systemic issues

affecting human rights and corruption. Naim writing on the topic states:

> Mafia states integrate the speed and flexibility of transnational criminal networks with the legal protections and diplomatic privileges enjoyed only by states, creating a hybrid form of international actor against which domestic law enforcement agencies have few weapons [2].

Using McCarthy-Jones and Turner's framework for delineating a mafia state, the Russian Federation appears to fit most closely with what they term a sub-type 3 mafia state in which the state is somewhat engaged with organised crime, is an authoritarian state with a controlled opposition, where all institutions are subservient to the political regime, the state allows select criminal and illicit behaviours/organisations and co-opts or utilises these in instances where it is of benefit to the state, and the state is capable of delivering public goods [1]. Åslund writing on the Russian government infrastructure refers to it as a kleptocracy [3]. Kleptocracy is broadly defined as a government or state which leverages the power of the state to steal or exploit national resources at the expense of those from whom it steals. Walker and Aten highlight that in some instances kleptocracy can extend beyond greed and can instead serve as a mechanism to gain geostrategic power that can undermine the stability of adversary, often democratic regimes. They refer to this as the 'weaponization of kleptocracy' [4]. Galeotti in writing on Russia's kleptocracy identifies Russia as a 'mobilization state' where all institutions, public or private, can be brought into the service of the state [5]. While frequently these types of criminal activities occur in physical spaces, they can also extend and spill over into digital spaces. Theft of information, the targeting of infrastructure, the undermining of information environments, and the use of ransomware can all bring geostrategic, intelligence, informational, and financial rewards to the mobilised kleptocracy. The challenge presented here is in delineating what is part of a mobilised kleptocracy and what is simply unaligned criminality. Whether using the term mafia state or kleptocracy, the result is the same, a state that leverages criminality for the gain of a government or individuals in positions of power in the state. What is unique about the Russian Federation is its ability to leverage its criminal–state networks for geopolitical gain across multiple dimensions.

This paper is principally concerned with how the Russian Federation mobilises, monitors, or controls its criminal elements in the service of the state as broadly defined. There appear to be two distinct

perspectives that are closely aligned, the use of proxies or the use of privateers. Early discussions of these two concepts were brought to the forefront by Klimburg, when he wrote extensively on cyber operations conducted by patriot hacker groups or loosely affiliated hacker organisations targeting opponents of the Russian or Chinese states [6]. Cases of patriotic hackers involved in serious cyber incidents are common. The principal cases associated early debates on Russian involvement in cyber actions through 'unofficial' actors begins with the 2007 distributed denial of service attacks against the Republic of Estonia [7] and the asymmetric use of cyber tools to degrade the communications of the Republic of Georgia during its short conflict with the Russian Federation in 2008 [8]. In the former case, Estonia was targeted not by the Russian state but rather through hacker groups with affiliated interests. This case proved particularly problematic for North Atlantic Treaty Organisation (NATO) and Estonia as noted by Egloff, because the speed of response from NATO and Estonia was unable to align with the challenges presented by the attacks themselves. Moreover, the attacks were not directly attributable to the Russian Federation, although significant involvement was suspected [9]. In the latter case, in which Russia invaded Georgia, there is ample evidence that criminal organisations, such as the Russian Business Network, played a substantial role in directing Distributed Denial-of-Service (DDoS) attacks or providing the resources to do so [8]. Despite substantial evidence of Russian involvement, again no conclusive evidence linked the actions of non-governmental Russian actors to the Russian state [10].

These two cases and many others that would arise in the decade to follow sparked research into the role and relationship of the state in cyber actions by non-state actors. Prominent among the research in this area was analysis conducted by Maurer on the concept of cyber proxies. Maurer defined a cyber proxy as 'an intermediary that conducts or directly contributes to an offensive action that is enabled knowingly, actively or passively, by a beneficiary' [11]. Maurer's notion of what constitutes a cyber proxy is expansive and legally difficult within the context of international law as demonstrated by Egloff [9]. Yet, Maurer builds a robust case for his expansive definition using examples of dropped prosecutions against hackers or insider comments on the visibility of the Russian state into its own networks (a concept discussed in more detail below) [11]. Maurer further finds that the relationship between Russia and its cyber proxies constitutes a conscious sanctioning (condoning) of actions targeting third parties [11]. He also notes, as will be demonstrated in subsequent sections, that the state has the capacity to stop such

actions but chooses not to [11]. The state chooses not to exert direct control on criminal actors because, as stated by Maurer, they are seen as beneficial to the state.

Martin and Whelan write that 'for the purpose of plausible deniability, the use of criminal proxies is ideal …' [12]. Yet, this is not entirely the case as demonstrated by Canfil using formal models expressing the concept of plausible deniability of cyber actions by proxies [13]. While it may be true that some actors are in fact proxies, this analysis agrees with Martin and Whelan in stating that proxies are generally most associated with actors that are politically aligned with and serve as an extension of the state [12]. Like Martin and Whelan, we also find that Egloff's concept of cyber privateers to be both provocative and intriguing in its ability to bridge the concepts of the kleptocratic state and the criminal enterprise [9]. Egloff's concept of privateers was further supported as an analogy by the work of Vostoupal and Uhlířová, who differentiate between the consequences that might befall a captured pirate versus a captured privateer [14]. In particular, leaning on their analysis and on Egloff's, we find traction in the historical precedent for undermining strategic adversaries through criminal activities defined by Egloff as piracy.

The key differentiation between the two activities is that where proxies have a more direct relationship with the goals and objectives of the state, the privateers are afforded greater leniency to interpret their mandate. While historically, the use of privateers was formalised through letters of marque, such a formal relationship between the state and the criminal entity would constitute a *de jure* consent that has not been demonstrated formally in the relationship between the state and cybercrime organisations.

Our data on ransomware attacks demonstrates that a disproportionate number of ransomware attacks likely originate with Russian actors. This is an important point because whether these actors are proxies or privateers is a legal and perhaps theoretical distinction. However, the next section explains the notion that these actions are occurring without state sanction unlikely.

3. Russia's Domestic Internet

Understanding Russia's involvement in its global cybercrime industrial complex begins by understanding the control that Russia exerts over its domestic Internet space and actors. Since 1993, the Russian Federation has been consistently tightening its control over its domestic Internet. State control over nearly

all aspects of the Internet has become ubiquitous since 2022 [15]. Restrictions and controls include the introduction of the System for Operative Investigative Activities (Система оперативно-разыскных мероприятий) – SORM 1 in 1995, SORM 2 in 2000, and SORM 3 in 2014 [16]. SORM provides extensive government surveillance of all domestic internet infrastructures, including Deep Packet Inspection (DPI). It published laws on the regulation of foreign agents 121-FZ, on blocking 'extremist websites' 139-FZ, data localisation laws 242-FZ, stored communications law 374-FZ, federal law on information and information technologies and information protection 276-FZ, law on the sovereign Internet 90-FZ, and multiple amendments to each of these laws further strengthening the power of the state in digital spaces [17–21]. Since February 2022, the Russian Federation took dozens of additional steps to penalise, censor, control, or restrict information and conduct in digital spaces within RuNet. By 2025, Russia's Internet authority, the Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor), was documented as having blocked hundreds of thousands of websites [22].

Russia has extensively prosecuted individuals deemed to be in violation of the above laws where those individuals challenge or otherwise threaten the narrative or security of the state or its perceived actions [23]. Russia has demonstrated a capacity and willingness to control the minutest details of its domestic Internet. Russia's capacity to control its domestic Internet is not isolated to its control over open web properties; rather, its control extends to control the use of virtual private networks (VPNs) [24], and the use of dark web services. Figure 1 shows the percentage of successful TOR connection attempts using Open Observatory of Network Interference data. The data in the figure indicates both a decline in accessibility of the TOR network and an overall general low accessibility of the services for the last 3 years.

Why should we care about Russia's domestic control over its Internet when discussing ransomware? Russia's extensive ability to block, control, surveil, and prosecute individuals for their online activities is extremely well documented. Russia has instituted what Stadnik refers to as 'control by infrastructure' [25]. This control includes deep-packet inspection, traffic monitoring, and more. All of this indicates infrastructure control with a capacity that far exceeds the ability to censor and control domestic speech. These capabilities suggest potential state visibility into domestic networks, though this visibility does not necessarily imply the ability or willingness to dismantle criminal ecosystems. Control seemingly does not fully

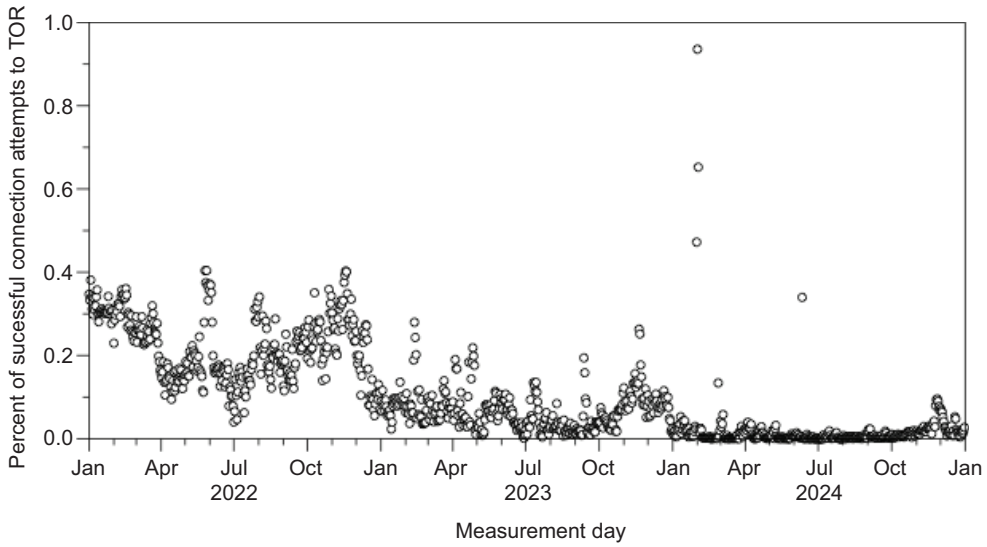

Figure 1. Percent of Successful Connection Attempts to Tor by Measurement Day.

extend to its criminal elements except where those elements target Russian entities [26]. The evidence indicates a significant underenforcement of laws related to ransomware domestically within the Russian Federation as well as a weakness in the utilisation of the existing international criminal laws under the existing international regimes [27]. All relevant facts indicate some sort of state–criminal interaction. As Canfil writes, there is an illogic to the plausible deniability espoused by the state in this instance [13].

4. The Russian State and Ransomware

As the two previous sections illustrate, there is a robust literature on the Russian crime and cybercrime industries. Russia is often identified as an example of a kleptocratic or mafia state. Yet, how can we reasonably establish Russian involvement in the absence of formal statements, letters of marque, or other direct attributions. The previous section establishes that the Russian RuNet is one of the most surveilled and censored domestic Internet spaces globally. There is a plethora of examples of individuals posting banal social media posts about the war in Ukraine being arrested. There are also examples of the weaponisation of legal and technical infrastructures in closing or shutting down entire swaths of digital infrastructure within the Russian Federation. Moreover, accounts from inside Russia and beyond demonstrate its extensive reach and control over nearly the entire digital infrastructure of the state [28].

Our argument is that the Russian state is passively and actively involved in ransomware and uses its criminal–state networks to augment its strategic and geopolitical objectives in a manner that has been significantly damaging to perceived adversary states and the businesses, organisations, and institutions within them. It has also been beneficial to the Russian state by providing financial capital inflows and technical talent to assist on more targeted cyber operations. Frequently these operations have been directly attributed to advanced persistent threat (APT) groups directly linked to the Russian Federation by other states [29], security threat groups, such as Microsoft [30], and the Ukrainian computer emergency response team [31]. Smeets documented a transition and professionalisation of ransomware activities to what he refers to as ransom war groups [32].

Ransomware's development into a state-sponsored cyber weapon did not happen overnight. Three major developments brought malware from a nuisance to the world-halting and multinational security threat that we know today. First, the development and commoditisation of cryptocurrencies enabled anonymous, near untraceable, and easily transferrable payments at scale [33]. Second, the shift to 'big game hunting' – the strategy of targeting major corporations over individuals – enabled hackers to concentrate less on proliferation and more on maximising damage, amplifying both financial gains and strategic impact. Third, the adoption of double-extortion tactics, where attackers not only encrypt data but also publish it on the dark web, created new forms of leverage over victims [34].

The ransomware landscape underwent a revolutionary shift in 2020, one that Bátrla and Harašta identify as a significant threat to Western states [35]. Both private and state-sponsored actors recognised the malware's potential as a tool of large-scale disruption and destruction. The COVID-19 pandemic's sudden onset forced businesses to quickly digitise their processes, creating new vulnerabilities. At the same time, the development of Ransomware-as-a-Service (RaaS) models enabled private and state-affiliated groups to significantly scale up their operations. The combined events created the perfect environment for ransomware to reach unprecedented levels of scale and damage. The healthcare industry saw an increase in attacks of nearly 40% from 2019 to 2020, and a staggering increase of nearly 600% in personal health information (PHI) leaks (from ~3 million to ~18 million) [36]. No industry was left unscathed by ransomware in 2020. Bitdefender reported a 485% increase in global ransomware reports in 2020, compared to 2019 [37].

The 2021 Colonial Pipeline attack exemplifies this evolution. When the Russian-affiliated group DarkSide attacked the billing system of America's largest fuel pipeline, they demonstrated Russia's potential to disrupt Americas largest fuel pipeline, the potential to disrupt critical infrastructure and create widespread panic among the American population [38]. The attack, which prompted fuel shortages across the US East Coast and a $5 million ransom payment from the company, highlighted how criminal ransomware groups and foreign adversaries have a symbiotic relationship – ransomware groups advance state interests while remaining protected, and countries retain some level of deniability [39].

Russian attitude towards ransomware reflects patterns with consistent state support and protection for this criminal enterprise. Pro-Russian groups enjoy systematic negligence from lawmakers and law enforcement, refusal of extradition requests from the United States, and direct state sponsorship with the stipulation that they must not target Russian interests and must occasionally assist in state objectives [40].

As private ransomware has undergone increasing development, governments have begun to recognise the disruptive and destructive power that this malware holds. Many countries, including the United States, Great Britain, and Australia, recognised the risk that ransomware poses to not only individuals but also small businesses, large corporations, and governments themselves. Europol's European Cybercrime Centre described ransomware as a 'top priority threat' and 'one of, if not the, most dominant threats, especially for public and private organisations within as well as outside of Europe' [41]. While many countries have been taking precautions to protect against ransomware and punish those who author and disseminate the malware, other countries have been taking an offensive approach. The governments of Russia, China, North Korea, and Iran have not only used ransomware as an offensive weapon, but through systematic negligence, refusal of extradition, and direct sponsorship, created a haven for cybercriminals, particularly those involved in ransomware [40].

Many of the largest attacks in the last 4 years are traced back to Russia. In terms of victims, Russian-affiliated ransomware strains make up the top three ransomware strains, five of the top 10, and 26 of the top 50 most impactful strains. In addition, while Russian-affiliated groups only make up 26% of the total publicised ransomware strains since 2020, they account for 63% of all attacks. This disproportionately high ratio can be traced back to Russia's

historically lax views on ransomware. Russia has continued to tighten their control over their Internet infrastructure, online content, and communication privacy, while the impact and scope of Russian ransomware continues to grow [42]. The laws and policies enacted by the Russian Duma and its digital infrastructure agencies tend to focus on constraining domestic actors from engaging in certain domestic activities, but places little in the way of limitations on their activities that extend beyond their borders. Russia's permissive legal environment for cyber activities, engaging foreign targets combined with an abundance of highly trained IT professionals, low wages and strong financial incentives, establishes the necessary conditions for cybercrime [43].

Ransomware groups took advantage of Russia's lax stance and occasional support of cybercrime. When a ransomware vendor's servers were seized by the Western authorities, an individual posted on dark web forum: 'Mother Russia will help … Love your country and nothing will happen to you' [44]. Essentially, the rule of thumb for hackers is that as long as you do not attack Russia or its interests, and occasionally help Russia in its own cyber agenda, you are free to hack whomever you want [44].

This transactional model between the state and these illicit organisations is not new. The early 20th century saw the Bolsheviks sponsoring bank robbers to rob banks to fund their government while not officially affiliating themselves with the robbers to maintain plausible deniability. The Stalin regime recruited organised criminals to keep political prisoners in line in the *gulags* [45]. Today, Russia's relationships with its cyber proxies are consistent with its use of proxies in non-cyber domains. The Federal Security Bureau (FSB), Russia's equivalent to the Federal Bureau of Investigation (FBI), sponsors many organised crime networks for money laundering, drugs and weapons trafficking, assassinations, and the exfiltration of compromised covert agents [12]. Organised crime and ransomware groups have a certain level of freedom in their operations, provided that at any time the state could demand covert service from any licit or illicit organisation or entity [45]. Private militaries, such as the Wagner group, have had claims of war crimes posed against them, deflecting the blame of Russia's actions to private entities [46]. What started as a necessity for staying functional in an early Russian state, Russia's relationship with organised crime has become a deeply ingrained function of Putin's government. Russia's relationship with ransomware groups is not a new phenomenon – it is merely an evolution of the state's steady transactional relationship with crime.

The top six Russian ransomware groups account for 56% of all global ransomware victims (7142 victims) in our dataset. Figure 2 illustrates the proportion of victims from 12 January 2020 through 22 April 2024, and includes data on attacks against 12,842 victims perpetrated by 110 identified ransomware groups. Yet, although the number of ransomware groups is large, the number distribution of attacks by group is highly consolidated to several key actors, most of whom are Russian in origin. Ransomware is a global problem with significant Russian origins. It is a means to harass and degrade the security of Western states through targeted and indiscriminate attacks against nearly every type of institution.

5. Hypotheses

To date, most studies take a case-based approach identifying the issue of Russian involvement in ransomware. These case studies can be extremely robust and include detailed information, including the number of victims of a given ransomware perpetrator. We find these studies helpful in understanding the nuances of the Russian sanctioned ransomware problem space. We found that Smeet's recent book, *Ransom war: How cyber crime became a threat*

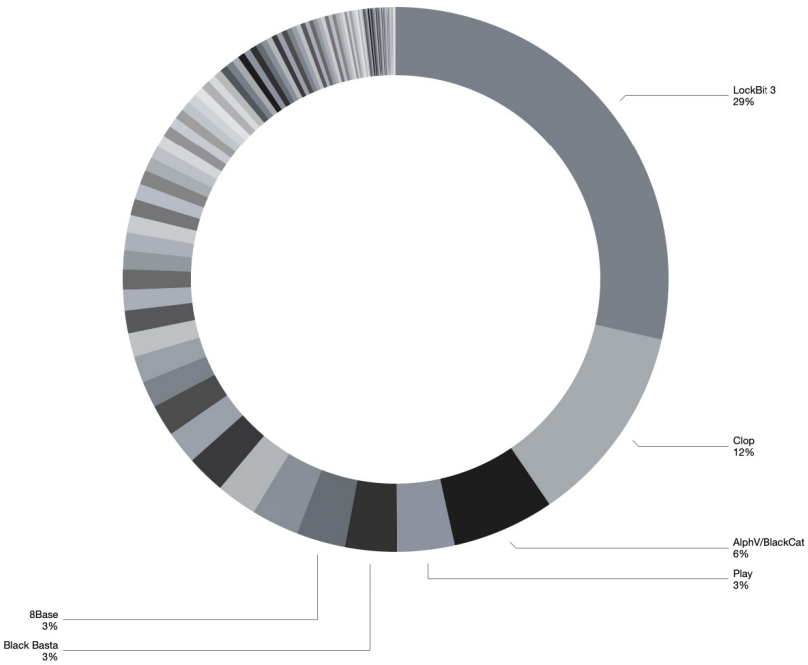

Figure 2. Proportion of victims by ransomware group affiliation for 7142 identified victims.

to national security, provided a detailed account of the relationship between the Conti Group, its spin offs, processes, and relationship with the Russian state [47]. We also found Smeet's analysis of the process of ransomware execution extremely detailed and helpful in understanding the process by which victims are selected and subsequently exploited. However, these studies do not fully explain the scope of Russian involvement within the global ransomware ecosystem. We wish to build on these case-based analyses with a data-driven analysis to provide additional context and add to the field's understanding of Russian involvement in global cybercrime.

Based on the logic of the criminal–state nexus developed in the first section and the permissive environment for Russian ransomware actors to operate, and the high level of technical capacity of Russian IT professionals, we hypothesise that the Russian state is likely to have a statistically significant percentage of ransomware market within our open-source dataset. If our hypothesis is confirmed, this would indicate both a capacity for ransomware development and action and a lack of due diligence on behalf of the state to mitigate criminal activities originating within the sovereign borders of a state [10]. Formally, our hypothesis states the following:

> Hypothesis H1: High-volume ransomware victimisation is likely to be disproportionately concentrated among Russian-affiliated groups within our open-source dataset.

We recognise that our data is subject to a variety of potential biases. Our data constitutes a subset of the population of all ransomware cases and may indicate an under counting of Russian victims. Although there is no evidence that supports this, as the collection of leak-site data is not done on a country-specific basis. While we believe that the volume and veracity of the dataset make the sample robust, it is also likely that there are imbalances within the identification of actors and affiliations within the data. While we have tried to engage in due diligence to verify affiliations and actors were possible not all ransomware attacks are attributable within our sample.

Further supporting our argument that there is both implicit and explicit Russian involvement in global ransomware, we build our second hypothesis on the relative attacks per country and believe that the number of ransomware attacks targeting entities within the Russian Federation is likely to be significantly fewer than those occurring in other states. This likely indicates a directionality of

attacks, and aligns with the hypotheses of proxy and privateering relationships, but does not help in differentiating them [11].

> Hypothesis H2: If the Russian state is involved through either proxy or privateering relationships, we expect there to be a directionality associated with ransomware attacks. This directionality manifests in a higher likelihood of entities external to the Russian Federation being targeted than entities internal to it.

> Because victim location is not observed for all incidents, H2 is evaluated on the subset of complete cases with observed victim location and attacker affiliation as defined within the RansomLook post collection.

> Combined with prior studies and case analyses, we believe that these two hypotheses establish a strong correlative relationship between global ransomware behaviour and the Russian state's sanctioning or involvement. This correlative relationship is likely to be demonstrated by both the substantial proportion of attacks within our dataset identified as being of Russian origin or affiliation and the directionality of ransomware incidents identified. The next section explains how we collected and subsequently analysed the data.

6. Methods and Results

In this section, we explain how we collected and evaluated data for our dataset. Moreover, we explain why this data is available and why there are potentially gaps in the data that arise.

The data in our dataset is largely self-produced by ransomware perpetrators. Ransomware groups have increasingly shifted towards double extortion methods that require them to share data to victims on blogs posted using Onion services within the Tor network. Ransomware as a criminal enterprise is different from many other forms of theft and requires a relationship predicated on trust between victims and perpetrators [48]. This trust is based on many factors, including reputation, a demonstration of control over data. Victims must trust the reputation of the perpetrator to unlock systems and delete files upon receipt of funds. Perpetrators must demonstrate that they possess the files and pose a credible threat. To establish a reputation among victims, ransomware groups use blog posts of containing redacted portions of a victim's data to

signal resolve. Groups often post private data from victims who do not pay ransoms. Blog posts often contain a variety of information types, including indicators of compromise, group names, instructions on how to pay a ransom, and more. Frequently, the sites hosting the stolen data also include chat forums that allow victims to communicate with perpetrators and ask questions. At times, perpetrators even provide samples of stolen files to the victims to demonstrate possession and resolve. While each victim often considers the interaction with the ransomware group to be a single interaction, the reality is that ransomware as a business model is more closely related to an iterative game [48]. As a result, interactions between perpetrator and victim are often public or accessible. For our initial foray into ransomware ecosystem, we sought out individual addresses through dark web forms, on dark web marketplaces, and on Telegram. We wrote several scripts to download and store data in a data repository. We ran into a number of data collection challenges, including advanced captchas, dead links, rate-limited sites, and more. We found that this process was inefficient and resulted in a sample of data that was smaller than we intended. Due to the inefficiency of seeking out data on a one-by-one basis, we instead turned to a publicly accessible aggregation site of ransomware data, called RansomLook, and used application protocol interfaces (APIs) from their service connected to an ElasticSearch server and Kibana dashboard to visualise data and create a downloadable database for subsequent analysis. Our resulting dataset ingested raw data and developed indices, such as attacks (victims), forums (where information on attacks or groups is shared), and groups (perpetrators of attacks). We recognise that the data is a sample of the overall population of ransomware attacks and likely does not represent all ransomware attacks, actors, or countries involved. However, these data are still useful in understanding the relationship between Russian- and non-Russian-affiliated ransomware criminal activities over the last several years.

At the time of writing, our dataset includes 19,128 ransomware attacks inclusive of 156 different ransomware types across eight different country identifications. Some of our data was pre-coded by RansomLook to include ransomware actor affiliation. This affiliation was made either through explicit language usage within ransomware sites and forums or via threat reports from vendors or governments. We augmented these designations through additional research on each ransomware group and added multiple other national ransomware affiliations by correlating ransomware group names on websites with industry threat reports. Figure 3 presents the top 50 ransomware groups by number of victims within

our sample. Several ransomware actors comprise the majority of all ransomware incidents within our dataset. LockBit3 is the most prominent within our dataset with 4021 victims.

7. Empirical Findings for Hypothesis 1

To test our first hypotheses, we ran a two-sample F-Test for Equality of Variances using groups. We coded all actors in our data as either 1 – Russian affiliation or 0 – no-Russian affiliation. Our F-statistic was 38.01. The variance in victim counts among Russian-affiliated groups is about 38 times larger than the variance among non-Russian groups. The mean number of victims within our data for Russian-affiliated actors was 252.93 across 43 different Russian-affiliated ransomware groups. By contrast, the mean number of victims of non-Russian-affiliated ransomware groups was 55.11. It should be noted that our data is skewed because of LockBit 3. We removed LockBit 3 as an outlier and reran our analysis. Among the 42 remaining Russian-affiliated groups, the average number of victims remained high at 163.2 victims per group. The F-statistic without LockBit 3 was 6.2. The variance of victim counts per group among Russian-affiliated groups (excluding LockBit3) is about 6.2× larger than the variance among non-Russian-affiliated groups. Second, we ran a Welch's two-sample t-test on the data by including and excluding LockBit 3. With LockBit3 included, the average Russian group appears massive (253 victims vs. 55). However, because LockBit3 is such an extreme outlier (4021 victims), it creates massive 'noise' (standard deviation) in the data. With LockBit3 included, the Welch t-test does not reject equality of means at (alpha = 0.05; p = 0.059). Excluding LockBit3, Russian-affiliated groups exhibit a significantly higher mean victim count (p = 0.016). When we remove the extreme outlier (LockBit3), the 'noise' in the Russian data decreases significantly. We can now see clearly that the average Russian group is still 3× more destructive (163 victims) than the average non-Russian group (55 victims). The p-value (0.016) confirms that this difference is real and not due to chance. Although LockBit 3 constitutes a dominant actor within the Russian ransomware ecosystem, it is not the sole driver of Russian dominance. The statistical significance of the Russian ecosystem's volatility is robust. The data suggests that the environment itself – likely due to safe harbour, resource sharing, or talent density – consistently produces high-impact actors (like Clop, Alphv, and BlackBasta) that outperform global norms, regardless of whether LockBit3 is included in the model. This is borne out in Figure 4, which provides a percentage distribution of actors. Large-scale perpetrators of ransomware attacks are statistically more likely to

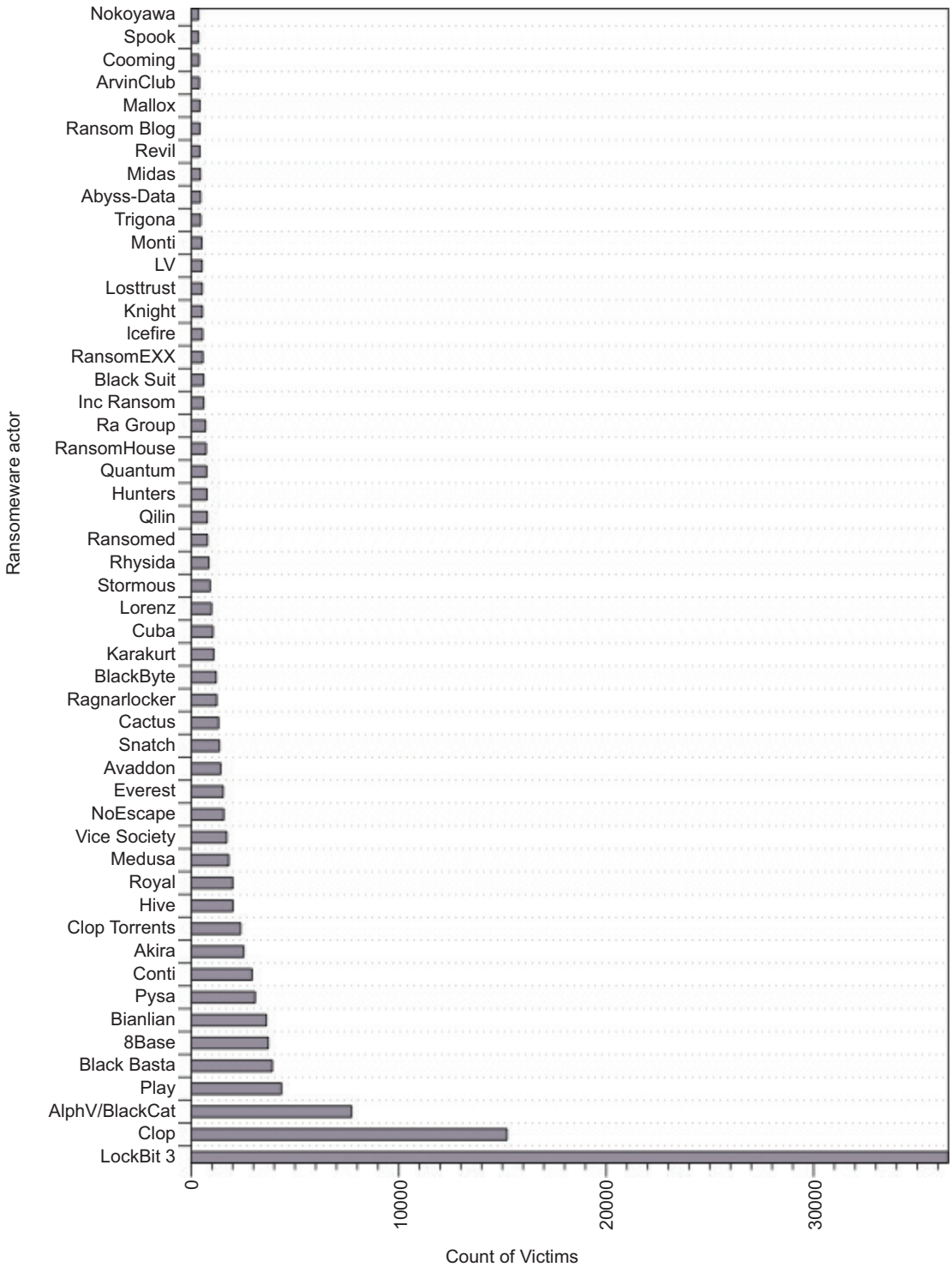

Figure 3. Top 50 ransomware groups by victim count.

be Russian-affiliated than any other affiliation. This significance is likely an underaccounting, as a very large percentage of the overall number ransomware actors are not attributed, meaning there is no corresponding state affiliation.

Having established that the overwhelming number of ransomware attacks within our data are Russian-affiliated, we turn to the directionality of ransomware attacks globally. Within our dataset, we have identified the full location of 6339 ransomware victims. Figure 5 provides a heatmap distribution of the victims. Among identified victims, the United States has 2793, followed by Canada at 586. The Russian Federation, by contrast, has only 17 documented victims within our identified victim set; 15 of the 17 victims were targeted by known Russian-affiliated ransomware group Werewolves, one was targeted by suspected Russian-affiliated Ransomware group funksec, and another victim was targeted by a ransomware group with no known affiliation. One notable detail is that 15 attacks within Russia were attributed to the Russian-affiliated Werewolves group. This group speaks Russian, which points to its members living in or near Russia. This ransomware group was extremely short lived, with the first posts being noted on 19 December 2023, and the last posts being noted on 12 February 2024. Notably, 15 of the 17 Russia-based victims in the geolocated subset are attributed

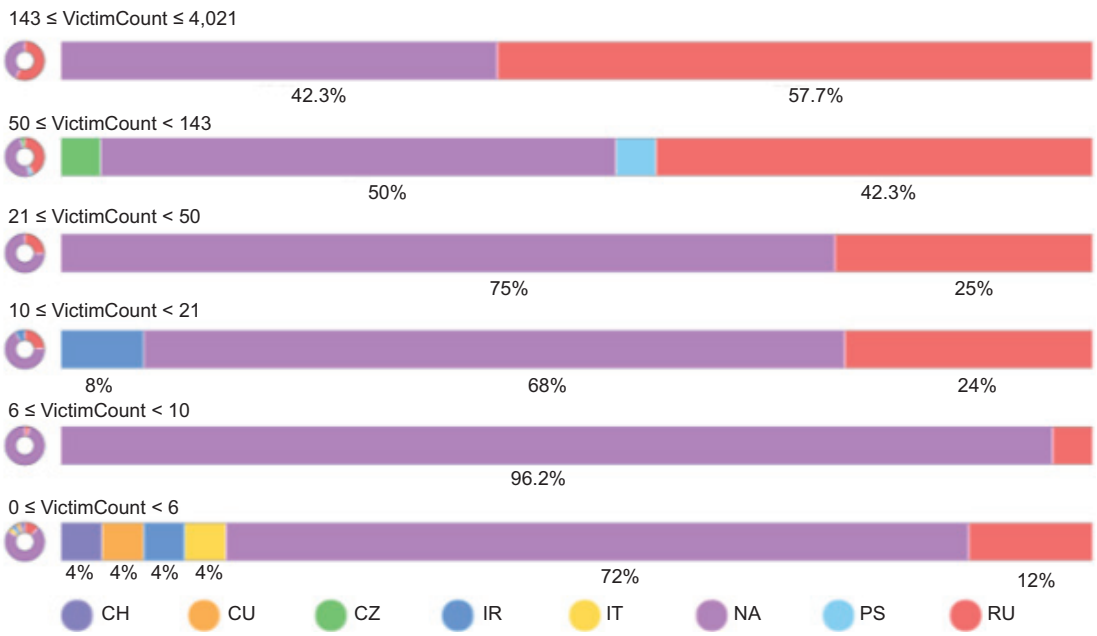

Figure 4. Ransomware national affiliation by number of victims.

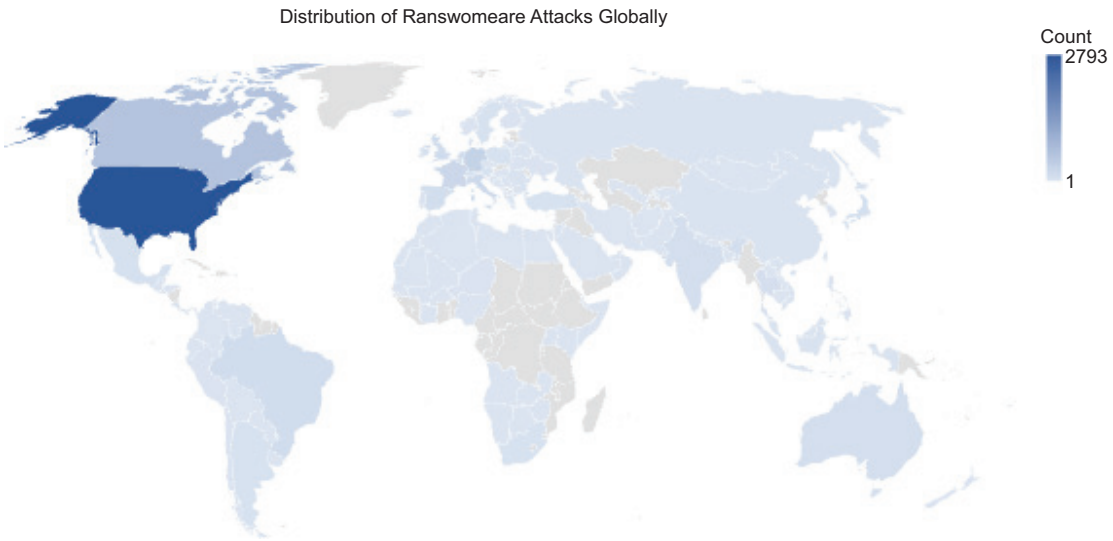

Figure 5. Distribution of ransomware attacks globally.

to the short-lived Werewolves group, whose leak-site activity in our collection spans from 19 December 2023 to 12 February 2024. The temporal proximity between domestic Russian targeting and the cessation of observable leak-site postings is consistent with (but does not establish) the reasonable possibility of enforcement pressure or operational disruption following domestic attacks. Alternative explanations – including rebranding, voluntary cessation, infrastructure disruptions, or observation gaps – cannot be ruled out with the present data. While state censorship could theoretically obscure domestic Russian victims, the business model of ransomware relies on publicising hacks to force payment. The absence of large volumes of Russian victims on these public leak sites is consistent with low domestic targeting, though suppressed reporting remains possible. Moreover, the criminological literature on Russia indicated above highlights the directional nature of Russian criminal activities towards targets beyond state borders.

8. Empirical Findings for Hypothesis 2

To test H2, we compared the domestic-targeting rate (victim in Russia) between Russian-affiliated and non-Russian-affiliated incidents in the complete-case subset. To assess whether Russian-affiliated ransomware is primarily externally directed, we first computed the share of Russian-affiliated incidents that target victims outside Russia. We then compared domestic targeting rates

(victim located in Russia vs. outside Russia) between Russian-affiliated and non-Russian attackers. Analyses are restricted to incidents with non-missing attacker affiliation and victim location (n = 6339) complete cases from (N = 19,128). Location data was provided within the RansomLook dataset. Location data is predicated for the attacker on location of the ransomware group as identified in posts or threat reports. Location data for the victim is identified by location of the named victim in posts.

Among Russian-affiliated incidents with observed victim location as identified within the RansomLook dataset (n = 2508), 99.52% target entities outside Russia (95% CI: 99.16%, 99.73%), and 0.48% target entities within Russia (95% CI: 0.27%, 0.84%) indicated overwhelmingly outward targeting. In the full complete-case sample (n = 6339), domestic Russian targeting remains rare (17 incidents; 0.27%) but occurs more frequently among Russian-affiliated attackers (0.48%) than among non-Russian attackers (0.13%). A Fisher's Exact test rejects independence (two-sided [p = 0.012]). Logistic regression yields an odds ratio of 3.68 (95% CI: 1.29, 10.46 (p = 0.015), with similar results under Firth penalised logistic regression (OR = 3.48, 95% CI: 1.28, 9.51 [p = 0.015]). These results indicate that, conditional on observed victim location, Russian-affiliated ransomware is overwhelmingly directed externally while also exhibiting a higher relative propensity to target Russia than non-Russian attackers within this observed subset.

9. Discussion

While Russia will likely never admit to a transactional relationship with crime on any level, a plethora of circumstantial evidence points to their key role in the success of ransomware originating from and around the country. Russia's foreign goals are reflected in where ransomware groups attack.

Filtering the database down to 42 groups with known or heavily implied ties to Russia presents a clearer picture of Russia's emerging ransomware strategy. Russia's hostility towards the United States is shown in full effect, with 2793 attributable attacks since 2020, making it the most targeted country by these groups. While the United States is certainly an outlier, many countries have seen their fair share of attacks and point to Russia's view of countries outside of cyberspace. Australia, Brazil, Canada, The Czech Republic, France, Germany, India, Italy, and Spain have individually experienced over 50 ransomware attacks at the hands of Russian-affiliated ransomware groups.

Interestingly, Russia's other adversaries have smaller attack numbers. The Russia–Ukraine war began in 2014 and intensified in 2022. Since 2021, 11 attacks by groups affiliated to the Russian government have been documented as attacking Ukraine. Eichensehr identifies that the lack of cyber action was unexpected [49]. Outside of one significant broadband attack and a handful of limited wiper and DDoS attacks, neither side has launched a large-scale cyber campaign against the other. Eichensehr discusses that Russia's poor planning, and an underestimation of Ukrainian forces, could have influenced the lackluster cyber campaign, or improved Ukrainian cyber defenses have kept more cyberattacks at bay, including aligning with the United States' 'defend forward' strategy and improved resilience in their power plants [49]. Most of the attacks documented against Ukraine by Russian-affiliated actors have targeted public administration, financial, and media assets and follow very much in line with attacks occurring during prior conflicts, in which the Russian Federation was a principal combatant [31]. Generally, these attacks have included ransomware like malware, but with the primary intent of exfiltrating data and subsequently wiping systems. The severity of cyber front in Russia's war with Ukraine did not match the predicted expectations [50]. Kostyuk and Gartzke suggest that cyber effects are insufficient to affect battlefield conditions significantly in a conventional war; rather they are most beneficial for achieving informational objectives [51]. Lin speculates that Russia's intent and lack of full utilisation of resources stems from its desire to save its best cyber tools for Western targets that offer greater strategic opportunity [52]. In Russia's eyes, support to Ukraine may be more costly than Ukraine's actions themselves. If they can cut aid off at the source, Russia may view that as a greater strategic opportunity [52].

What the overall weight of both circumstantial evidence from cases and our data-driven analysis from our dataset on victims by ransomware group, combined with the tightly controlled domestic Internet space of the Russian Federation, point towards patterns consistent with a tolerance for and permissiveness and directionality of ransomware emanating from Russian-affiliated actors. Our data analysis above and the case studies establish a core concept in the study of ransomware. The global ransomware problem is predominantly a Russian ransomware problem. The Russian state fails on nearly every level, seemingly deliberately, to engage in due diligence in only one aspect of its domestic network infrastructures, cybercrime that targets foreign – that is non-Russian entities. This finding has been articulated in legal analysis of the Russian cybercrime ecosystem through case analysis [10] and is supported by our data and analysis above.

10. Conclusions

The overwhelming evidence from both prior case analyses and the quantitative data presented above suggests that the Russian Federation either by proxy or privateer, or other form of sanction, formal and informal, uses ransomware as an instrument with potential geopolitical effects. Russia's ties within our data to over 11,000 recorded attacks underscore the alignment between cybercriminal activities and the country's political agenda. To date, our data suggests that the United States has taken the brunt of these attacks, which in many ways reflect the tumultuous relationship between the two nations. The ever-evolving nature of ransomware and its political implications require a coordinated global effort to improve and enhance cybersecurity measures, defences, and legal actions against ransomware. For governments, private companies, and NGOs, this threat is too large and too powerful to ignore. Whether states follow the call by Bátrla and Harašta to 'release the hounds' and empower cyber operations to counter ransomware [35] or whether they follow the logic expressed by Lubin to make more substantial use of the existing international legal structures to constrain and prosecute cybercrime [27], there remains an urgent need to address the issue. By highlighting Russian Federation-affiliated concentration patterns from our database of observed leak-site data, we are disambiguating the current ransomware crisis and taking accountability partially away from victims and reassigning it to the perpetrators and their protector.

References

[1] A. McCarthy-Jones, M. Turner, "What is a 'mafia state' and how is one created?," *Police Studies*, vol. 43, pp. 1195–1215, 2022, doi: 10.1080/01442872.2021.2012141.

[2] M. Naim, "Mafia states: Organized crime takes office," *Foreign Affairs*, vol. 91, pp. 100–111, 2012.

[3] A. Åslund, *Russia's crony capitalism*: *The path from market economy to kleptocracy.* New Haven, CT: Yale University Press, 2019.

[4] C. Walker, M. Aten, "The rise of kleptocracy: A challenge for democracy," *Journal of Democracy*, vol. 29, pp. 20–24, 2018.

[5] M. Galeotti. (2017). *Stolypin: Adding spooks to companies creates stagnation*. [Online]. Available: https://www.intellinews.com/stolypin-adding-spooks-to-companies-creates-stagnation-119924/ [Accessed: Feb 19, 2025].

[6] A. Klimburg, "Mobilising cyber power," *Survival*, vol. 53, pp. 41–60, 2011.

[7] C. Bronk, *Cyber threat: The rise of information geopolitics in U.S. National Security*. Santa Barbara, CA: Praeger, 2016.

[8] D.V. Puyvelde, A. Brantly, *Cybersecurity: Politics, governance and conflict in cyberspace*, 2nd ed. Cambridge: Polity Press, 2024.

[9] F. Egloff, *Semi-state actors in cybersecurity.* New York, NY: Oxford University Press, 2022, doi: 10.1093/oso/9780197579275.001.0001.

[10] T. McDougal, "Establishing Russia's responsibility for cyber-crime based on its hacker culture," *Brigham Young University International Law & Management Review*, vol. 11, pp. 55–80, 2018.

[11] T. Maurer, *Cyber mercenaries: The state, hackers, and power*. Cambridge: Cambridge University Press, 2018.

[12] J. Martin, C. Whelan, "Ransomware through the lens of state crime: Conceptualizing ransomware groups as cyber proxies, pirates, and privateers," *State Crime Journal*, vol. 12, pp. 4–28, 2023, doi: 10.13169/statecrime.12.1.0004.

[13] J.K. Canfil, "The illogic of plausible deniability: Why proxy conflict in cyberspace may no longer pay," *Journal of Cybersecurity* vol. 8, Art. no. tyac007, 2022, doi: 10.1093/cybsec/tyac007.

[14] J. Vostoupal, K. Uhlířová, "Of hackers and privateers: The possible evolution of the problem of cyber-attribution," *Masaryk University Journal of Law and Technology,* vol. 18, pp. 169–214, 2024, doi: 10.5817/mujlt2024-2-2.

[15] K. Ermoshina, B. Loveluck, F. Musiani, "A market of black boxes: The political economy of Internet surveillance and censorship in Russia," *Journal of Information Technology and Politics,* vol. 19, pp. 18–33, 2022, doi: 10.1080/19331681.2021.1905972.

[16] J. Sherman. *Russia's digital tech isolationism: Domestic innovation, digital fragmentation, and the Kremlin's push to replace Western digital technology,* The Atlantic Council, Washington, DC, 2024. [Online]. Available: https://dfrlab.org/2024/07/29/russias-digital-tech-isolationism/. [Accessed: Sep. 8, 2024].

[17] International Center for Not-For-Profit Law. (2025). "Civic Freedom Monitor", International Center For Not-For-Profit Law. [Online]. Available: https://www.icnl.org/resources/civic-freedom-monitor/russia. [Accessed: Mar. 29, 2026].

[18] K. Koroleva. (2016). *"Yarovaya" law – new data retention obligations for telecom providers and arrangers in Russia*. [Online]. Available: https://www.globalprivacyblog.com/2016/07/yarovaya-law-new-data-retention-obligations-for-telecom-providers-and-arrangers-in-russia/. [Accessed: Sep. 9, 2024].

[19] A. Litvinenko, "Re-defining borders online: Russia's strategic narrative on internet sovereignty," *Media and Communication*, vol. 9, pp. 5–15, 2021, doi: 10.17645/mac.v9i4.4292.

[20] K. Lally. (2012). 'Russia passes law that could curb Internet usage', *The Washington Post*. 11 Jul. 2012. [Online]. Available: https://www.washingtonpost.com/world/europe/russia-passes-law-curbing-internet/2012/07/11/gJQAvkzPdW_story.html. [Accessed: Sep. 9, 2024].

[21] Meduza. (2020). *What you need to know about Russia's updated "foreign agent" laws.* [Online]. Available: https://meduza.io/en/feature/2020/12/28/what-you-need-to-know-about-russia-s-updated-foreign-agent-laws. [Accessed: Sep. 8, 2024].

[22] FreedomHouse, *Russia freedom on the net 2023*. Country Report, 2023. [Online]. Available: https://freedomhouse.org/country/russia/freedom-net/2023. [Accessed: Sep. 4, 2024].

[23] D. Litvinova, *The cyber gulag: How Russia tracks, censors and controls its citizens*, AP News, 2023. [Online]. Available: https://apnews.com/article/russia-crackdown-surveillance-censorship-war-ukraine-internet-dab3663774feb666d6d0025bcd082fba. [Accessed: May 23, 2023].

[24] C. Castro, 'Russia blocks almost 200 VPN services, but the Kremlin still wants to use them', *TechRadar*, 2024. [Online]. Available: https://www.techradar.com/pro/vpn/russia-blocks-almost-200-vpn-services-but-the-kremlin-still-wants-to-use-them. [Accessed: Feb. 17, 2025].

[25] I. Stadnik, "Control by infrastructure: Political ambitions meet technical implementations in RuNet," *First Monday*, vol. 26, no. 5, 2021, doi: 10.5210/fm.v26i5.11693.

[26] R. Dremliuga, O. Dremliuga, P. Kznetsov, "Combating the threats of cybercrimes in Russia," *Communist and Post-Communist Studies*, vol. 53, pp. 123–136, 2020.

[27] A. Lubin, "The law and politics of ransomware," *Vanderbilt Journal of Transnational Law*, vol. 55, pp. 1177–1216, 2022.

[28] A. Soldatov, I. Borogan, "The red web: The struggle between Russia's digital dictators and the new online revolutionaries," *Public Affairs*, 2015.

[29] Cybersecurity and Infrastructure Security Agency (2025). *Russian GRU Targeting Western Logistics Entities and Technology Companies.* [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa25-141a. [Accessed: Feb. 20, 2026].

[30] Microsoft. (2022). *An overview of Russia's cyberattack activity in Ukraine*. [Online]. Available: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK. [Accessed: Apr. 27, 2022].

[31] A.F. Brantly, N.D. Brantly, "The bitskrieg that was and wasn't: The military and intelligence implications of cyber operations during Russia's war on Ukraine," *Intelligence and National Security*, vol. 39, pp. 475–495, 2024, doi: 10.1080/02684527.2024.2321693.

[32] M. Smeets, *From ransomware to ransom war the evolution of a solitary experiment into organized crime*, Report, Cyberdefense, Space and AI, ETH Zurich: Center for Security Studies, 2024.

[33] G. Peters, *Use of cryptocurrency in ransomware attacks, available data, and national security concerns*. Committee on Homeland Security and Government Affairs, United States Senate, Washington, DC, 2022. [Online]. Available: https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf. [Accessed: Feb. 4, 2025].

[34] I.A. Chesti, M. Humayun, N.U. Sama, N. Jhanjhi, "Evolution, mitigation, and prevention of ransomware, 2020," in *2nd International conference on computer information science (ICCIS)* Sakaka, Saudi Arabia, 2020, pp. 1–6, doi: 10.1109/iccis49240.2020.9257708.

[35] M. Bátrla, J. Harašta, "'Releasing the Hounds?' Disruption of the ransomware ecosystem through offensive cyber operations," in *2022 14th International conference on cyber conflict: Keep moving (CyCon)*, T. Jančárková, G. Visky, I. Winther, Eds. Tallinn: NATO CCDCOE Publications, 2022, pp. 93–115. Available: https://doi.org/10.23919/CyCon55549.2022.9811074.

[36] H.T. Neprash, C.C. McGlave, D.A. Cross, B.A. Virnig, M.A. Puskarich, J.D. Huling, A.Z. Rozenshtein, S.S. Nikpay, "Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016–2021," *JAMA Heal. Forum*, vol. 3, Art. no. e224873, 2022. doi: 10.1001/jamahealthforum.2022.4873.

[37] Bitdefender. (2020). *Mid-year threat landscape report 2020*. [Online]. Available: https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf. [Accessed: Mar. 29, 2026].

[38] Colonial Pipeline. (n.d.). *About us*. [Online]. Available: https://www.colpipe.com/about-us/. [Accessed: Jan. 7, 2025].

[39] D.E. Sanger, C. Krauss, N. Perlroth, "Cyberattack forces a shutdown of a top U.S. pipeline," *New York Times*, [Online]. Available: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html. [Accessed: Mar. 29, 2026].

[40] H. Gately, *Russian organised crime and Ransomware as a Service: State cultivated cybercrime.* Sydney: Department of Security Studies and Criminology, Macquarie University, Institutional Author: EUROPOL. 2023.

[41] Internet Organized Crime Threat Assessment (IOTCA), 2020. (2021). EUROPOL. [Online]. Available: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2020. [Accessed: Mar. 21, 2026].

[42] Human Rights Watch. (2020). *Russia: Growing internet isolation, control, censorship*. [Online]. Available: https://www.hrw.org/news/2020/06/18/russia-growing-internet-isolation-control-censorship. [Accessed: Feb. 20, 2025].

[43] A. Jackson, "How the collapse of the Soviet Union made Russia a great cyber power," *The Cyber Defense Review*, Spring. pp. 99–112, 2024.

[44] A. Charlton, "How the Kremlin provides a safe harbor for ransomware," *AP News*, 2021. [Online]. Available: https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d-93ed3102999. [Accessed: Feb. 1, 2025].

[45] M. Galeotti. (2024). *Gangsters at war – Russia's use of organized crime as an instrument of statecraft*, Global Initiative Against Terrorism and Crime, Geneva. [Online]. Available: https://globalinitiative.net/analysis/gangsters-at-war-russias-use-of-organized-crime-as-an-instrument-of-statecraft/. [Accessed: Mar. 29, 2026].

[46] N. Camut, "Ex-Wagner officer says Kremlin ordered 'atrocities' in Ukraine", *Politico*, 2023 [Online]. Available: https://www.politico.eu/article/ex-russia-wagner-officer-russia-atrocities-ukraine-war-crimes-igor-salikov/. [Accessed: Feb. 4, 2025].

[47] M. Smeets, *Ransom war: How cyber crime became a threat to national security*, 1st ed. Oxford: Oxford University Press, 2025.

[48] A. Cartwright, E. Cartwright, "Ransomware and reputation," *Games*, vol. 10, Art. no. 26, 2019. doi: 10.3390/g10020026.

[49] K.E. Eichensehr, "Ukraine, cyberattacks, and the lessons for international law," *American Journal of International Law Unbound (AJIL Unbound)*, vol. 116, pp. 145–149, 2022, doi: 10.1017/aju.2022.20.

[50] N. Kostyuk, A. Brantly, "War in the borderland through cyberspace: Limits of defending Ukraine through interstate cooperation," *Contemporary Security Policy*, vol. 43, pp. 498–515, 2022, doi: 10.1080/13523260.2022.2093587.

[51] N. Kostyuk, E. Gartzke, "Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine," *Texas National Security Review*, vol. 6, no. 3, pp. 113–126, 2022.

[52] H. Lin "Russian cyber operations in the invasion of Ukraine," *The Cyber Defense Review*, vol. 7, no. 4, pp. 31–46, 2022. [Online]. Available: https://www.jstor.org/stable/48703290. [Accessed: Mar. 29, 2026].