Russian organised crime and Ransomware as a Service: state cultivated cybercrime

Hannah Gately

Bachelor of Commerce, Master of Cyber Security

Thesis presented to Faculty of Arts

Department of Security Studies and Criminology

Macquarie University

17 October 2022

Table of Contents

Abstract

Ransomware as a Service (RaaS) has become one of the most significant threats within the cybersecurity landscape, with a ransomware attack occurring every eleven seconds. Despite the growing awareness around RaaS within the cybersecurity community, there is currently a lack of research regarding the factors that have contributed to its growth, specifically, the factors that have contributed to the cultivation of RaaS within Russia by the Russian state. The thesis seeks to review the evolution of Russian organised crime from its beginnings in the USSR to its growth into the leading player within the RaaS space whilst examining Russian politics' role in this evolution. Furthermore, Russian ransomware's history and rapid development are examined, notable landscape shifts are identified, and their connection with the state are explored. The thesis will discuss the historical, socio-technical, and political influences that have contributed to the growth of Russian organised RaaS groups and the implications of these influences within Russia. The value of this work is to inform and educate those within the cybersecurity community on the factors influencing the rapid growth of RaaS, highlight where the RaaS threats originates and emphasise the non-technological influences of cybercrime offending.

Statement of Originality

This work has not previously been submitted for a degree or diploma in any university. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Hannah Gately Date: 17/10/2022

Introduction

1.1 Background

Within the cyber landscape, there is no threat that has grown the fastest (Grobman and Cerra, 2016) and has been more damaging than ransomware. A type of malicious software popular amongst Russian cybercriminals (Richardson and North, 2017), ransomware allows cybercriminals to encrypt an individual's or organisation's data, rendering it inaccessible unless a ransom is paid (Hassan, 2019). In 2021 the Australia Cyber Security Centre received almost 500 reports of ransomware, an increase of fifteen per cent from the previous year (Australian Cyber Security Centre, 2021). This number is expected to grow by an anticipated thirty per cent increase by 2025 (Kerner, 2022), an overall, concerning trend for cyber security experts. While ransomware has played a significant role within Russia, the software poses a considerable risk globally; a key aspect within the ransomware landscape poses a massive threat to global cyber security; Ransomware as a Service (RaaS).

RaaS is a criminal business model whereby ransomware is leased out by malicious software developers to affiliates to utilise (Kost, 2022). RaaS like traditional software as a service (SaaS), RaaS aims to democratise solutions by giving smaller players an easier way to enter the market while reducing the risk to those at the top of the pyramid (Meland et al., 2020). With its low technical barrier of entry, its potential for creating massive earnings for criminal developers and affiliates (Kost, 2022) and its ability to damage critical systems, businesses and reputations (Grimes, 2021), RaaS is the greatest threat to modern cyber security. However, while there has been significant research into ransomware, far less is known about RaaS and the factors contributing to its growth within Russia. RaaS has had a substantial impact on all global sectors, most distinviely health, infrastructure, and private enterprise; therefore, it is essential to understand the malware and influences that have allowed it to grow within Russia.

The concepts of ransomware and RaaS are nothing new within the cyber landscape, with Young and Yung (1996) presenting the concept of *cryptoviral extortion* in the mid-1990s. However, they are concepts that have evolved into one of the most damaging forms of cybercrime RaaS is a software package model that enables

"affiliates" or users to pay to utilise existing ransomware tools to execute attacks (Hassan, 2019; Kost, 2022). Shifting the development of malware tools to a third party has allowed for the diversification of those conducting effective ransomware attacks (Meland et al., 2020), all while providing organised ransomware groups with the ability to take a percentage of the profits. Since it was first utilised in the 1980s, ransomware has continuously adapted to new technologies and changes within the digital landscape. RaaS has provided organised cybercrime groups with the ability to generate profits through new methods and additional layers of extortions that were impossible just a decade ago. While early versions of ransom, such as CryptoLocker, accumulated a profit of $3 million (Groot, 2022), RaaS groups have accrued hundreds of millions of dollars, with one RaaS group, Conti reaping $180 million in 2021 (Sjouwerman, 2022).

RaaS has become one of the most damaging threats globally. Posing risks to financial, public and physical safety, the threat of RaaS dominates the cybercrime landscape more than any other malware (Europol, 2021; Verizon, 2022). While the average price of RaaS kits ranging from $40 to thousands, the profits obtained by RaaS groups are significant, with the average ransom demand totalling $6 million in 2021 (Baker, 2022). However, the overall cost of ransomware attacks and RaaS goes beyond just the ransom, with damages to reputation, system downtimes and legal fees costing far more than the ransom (BlackFrog, 2022).

While RaaS is a global threat, one state plays a substantial role in the history and development of ransomware and RaaS: Russia. As prolific players within RaaS, Russian threat actors were linked to 74 per cent of ransomware attacks in 2021 (Tidy, 2022). Furthermore, Russian RaaS groups have led the way in developing ransomware programs, including *Maze* and *BlackCat*, and ransomware Tactics, Techniques and Procedures (TTP) such as intrusion and exploitation methods. With their advanced organised cybercrime operations, Russian RaaS groups have become the definitive leader of ransomware.

1.2 Research Overview

This research project aims to identify why Russia has become a haven for RaaS and evaluate how the political-criminal nexus and socio-technical lens can further explain

this phenomenon. Specifically, this research aims to answer the question, how has the Russian state facilitated the growth of RaaS within Russia? This research project intends to identify the specific factors that have caused the development of organised ransomware groups within Russia. The particular aims of this research are to:

- Examine the role of the Russian government in the growth of RaaS.
- Analyse the socio-technical factors contributing to the adoption of RaaS.
- Identify the influences contributing to Russian organised crimes' utilisation of RaaS.

While ransomware research is a new domain, its usefulness involves multidisciplinary expertise (Broucek, 2006), combining aspects of criminology, psychology, cybersecurity, and economics. Significant research has been conducted on the evolution of ransomware (Hassan, 2019; Hughes, 2016; O'Kane et al., 2018), mitigation strategies for ransomware (Furnell and Emm, 2017; Mohanta et al., 2018), the role of RaaS in the darknet (Meland et al., 2020) and investigations into specific forms of ransomware. Previous academic work has also explored the economic modelling behind ransomware and the tools used to conduct ransomware activities, including Bitcoin and other cryptocurrencies. Additionally, previous scholarship has highlighted the connection between Russian and ransomware groups (Hassan, 2019; Richardson and North, 2017). However, there currently exists a gap within the research regarding the factors influencing this connection and the state's role in creating an environment for RaaS to flourish.

This research project fills the gap in the current research by looking at the Russian state's influence on the cultivation of RaaS in the nation. Rather than restricting the examination of RaaS through a purely technical lens which previous literature has primarily tended to do, it explores the causes behind Russia's adoption of ransomware through a political and socio-technical perspective (Yip et al., 2012; Broadhurst et al., 2013). Through examining Russia's adoption of RaaS through a lens that incorporates Russia's political landscape as well as the technological history and socioeconomics of the state, a more profound comprehension of the factors that have influenced the growth of RaaS within Russia. Specifically, through the utilisation of the political and socio-technical lens, the state's role in the

cultivation of RaaS as the approach provides greater insight into the nuances created by the Russian state that have influenced Russian organised crime's adoption of RaaS and the scale of these nuances. Additionally, using the political and socio-technical lens assists in developing a more robust understanding of why organised crime groups adopt certain cybercrimes, specifically why Russian organised crime groups have adopted RaaS compared to other organised crime groups.

Identifying the influences that contributed to the rise of RaaS in Russia could support several facets of the cybersecurity landscape. Cybersecurity researchers must remain aware of the current trends within the space. Therefore, awareness regarding the growth and changes within the Russian RaaS is essential. This research project can assist in future investigations regarding RaaS and ensure that the cybersecurity community can identify future trends within the Russian cybercrime landscape. Furthermore, in the cybercrime domain, a deeper understanding of the factors contributing to the adoption of cybercrime is essential. By examining cybercrime utilising the political-criminal nexus and socio-technical lens, this research can assist future criminology research on the motivations of organised cybercriminals.

1.3 Methodology

As this research project aims to identify the contributing factors behind the rise in Russian RaaS beyond just a technical approach, this project utilises the literature review. Through the review of materials including peer-reviewed journal articles, government reports, and materials from leading organisations and individuals within cybersecurity, the ability to consolidate existing research is possible. Evaluating sources from academic and private subject matter experts aided in providing a holistic and current evaluation of RaaS, Russian organised crime, the Russian political landscape, and the socioeconomics of the state. Furthermore, reports from government entities and leading cybersecurity firms provided instrumental analysis of Russian threat actors' role in the organised cybercrime landscape over the last two decades. To effectively identify relevant literature that should be included within the thesis literature coding was utilised. Through the use of literature coding a logical constructed and coherent position is possible and clear themes are established. For example, the thesis begun by searching for key words, including ‘RaaS’, ‘Russian

organised crime', and 'Russian cybercrime' before focusing on more specialised codes including 'Conti Ransomware', 'botnets', 'cryptocurrencies', 'Russian cyber warfare, and 'state-sponsored hacking'.

As argued by Snyder (2019), among others, the use of the literature review has its limitations. The potential to build flawed assumptions and form a rudimentary understanding of the arguments made in the collection of studies may hinder the overall accuracy of a study. Other methods of research were considered based on these limitations inclding the case study which may have reduced the risk of assumptions and provided insight into specific ransomware groups, however, due to time restraints it was not chosen. Nonetheless, the literature review was chosen for this research project because of its power to provide a comprehensive overview of a multidisciplinary research topic, its ability to synthesise the gaps within the current literature, and its ability to build upon current concepts relating to the research topic. Furthermore, as argued by Patten and Newhart (2018) as a rigorous research method, the literature review assists researchers in framing their research, which in turn allows for a more detailed introduction to empirical research regarding the relationship between RaaS and the Russian state.

1.4 Thesis Structure

The thesis is organised into four chapters. The first chapter explores the evolution of Russian ransomware and RaaS. This chapter identified that ransomware has been utilised consistently by Russian-based threat actors and showed that the shift of ransomware to a business model was a logical step made by Russian organised cybercrime groups. In the second chapter, the history of Russian organised crime groups is explored. The chapter shows that aspects of Russian organised crime's evolution contributed to their adoption of RaaS. This chapter highlights the significant role of the political-criminal nexus in Russian organised crime's development and its evolution towards RaaS. The third chapter examines Russia's political ecosystem and the role of the Russian government in cultivating RaaS. This examination identified that the political-criminal nexus has contributed to the growth of RaaS in Russia through the government's support of state-sponsored cybercrime. In the fourth and final chapter, the socio-technical lens is utilised to explore the factors contributing to Russia's adoption of RaaS. Analysis from this chapter shows that

specific aspects of Russia's technical history and socioeconomics have caused RaaS to flourish in the state. The chapter also examines why Russia has an environment that favours RaaS over other forms of cybercrime.

Russian Ransomware and the Rise of RaaS

RaaS has seen significant growth over the last five years, with cybersecurity authorities in Australia, the United States and the United Kingdom reporting an increase in the sophistication and impact of ransomware globally (Joint Cybersecurity Advisory, 2022). In Australia alone, the Australian Cyber Security Centre saw a 15 per cent increase in instances of ransomware between 2021 and 2020 (Lai, 2022). This chapter explores Russian ransomware's evolution from humble beginnings into the massive global threat of RaaS. The chapter also examines the broader aspects that have influenced the evolution of ransomware and the shift of ransomware to a business. A recurrent trend within the chapter will be the role of the Russian state in the evolution of Russian ransomware and RaaS.

As stated, ransomware is not a new concept within the cyber landscape, with academics discussing the idea of cryptoviral extortion in the 1990s (Young and Yung, 1996). However, while the concept is not new, this chapter proposes that three specific aspects of the evolution of Russian-based ransomware have contributed to the growth of Russian RaaS; the rise of new technologies, the shift of the role of the Russian state within the ransomware landscape, an increase in scalability and level of harm, and the rise of more precise programs. As the prevalence of RaaS groups increases; with a 139 per cent increase year-over-year (Kost, 2022), and the threat they pose globally grows, it is essential to substantiate the factors within the history of ransomware, most notably new technology and the role of the state in contributing to the rising appeal of RaaS in Russia.

2.1 Early Russian Ransomware

2.1.1 AIDS Trojan and the Beginning of Ransomware

While the chapter will focus solely on Russian-based ransomware and the factors that have contributed to its adoption by organised cybercrime groups, it is essential to explore the very beginnings of ransomware to ensure a comprehensive understanding of not only the history of the malware but also Russian organised cybercrime's and the state’s role within the landscape. Modern Russian ransomware programs are a significant threat on a global scale, with thirty-five per cent of businesses globally becoming victims of ransomware in 2020 (Birch, 2021); however, these programs started from unassuming beginnings.

The first reported case of ransomware was created in the United Kingdom in 1989 and was dubbed the "*AIDS Trojan*". This ransomware was delivered by floppy disks titled "AIDS Information – Introductory Diskettes" to roughly 20,000 individuals registered on the World Health Organisation's AIDS conference mailing list (Hassan, 2019). Through the utilisation of social engineering techniques, the individuals believed the disk contained a survey that could determine the risks of contracting AIDS; however, once inserted into their device, malware encrypts their hard drive, preventing access to the device's files (Mujezinovic, 2021). That was unless the user sent a payment of USD$189 to an address in Panama (Ahn et al., 2017; Hassan,

2019; O'Kane et al., 2018). Arguably, the *AIDS Trojan* impact was not significant on a grand scale due to its limited victim scope, weak encryption, and poor infection method (Ahn et al., 2017; O'Kane et al., 2017). However, the incident was at the forefront of the looming change within the cybercrime landscape.

As explored by Young and Yung (1996), the *AIDS Trojan* had planted the seeds of the potential of "data kidnapping", and the tangible threat cryptoviruses were to the confidentiality, integrity, and accessibility of data. Following the *AIDS Trojan*, there would be little ransomware activity until a resurgence of the malware in the 2000s. Between 2004 and 2006, several significant Russian ransomware programs entered the landscape - *MayArchive*, *GPCoder* and *Cryzip* (Nadir and Bakhshi, 2018). These ransomware programs would follow the same steps as the *AIDS Trojan*; infect a user's device, encrypt the user's files and demand payment to decrypt (Gazet, 2010; Giri and Jyoti, 2006; Hassan, 2019; Kawamoto, 2006); however, *MayArchive*, *GPCoder* and *Cryzip* were just the beginning of what would become the boom of Russian-based ransomware and eventually the rise of RaaS.

2.1.2 Russian Ransomware on the Rise

The early growth of Russian-based ransomware can be primarily attributed to the rise of new technology, specifically the development of botnets, the introduction of the ability to tailor code to fit the criminal's needs and the rise of cryptocurrencies. These new technologies gave Russian ransomware a new sense of scale, greater flexibility and precision and the ability to profit securely.

Botnets are a system of computers that a cybercriminal or 'botmaster' has commandeered to harness the power of a network of computers to conduct illicit activities, including ransomware (Grabosky, 2016). As tool that facilitates cybercrime, botnets provide cyber threat actors with a larger pool of potential victims due to increased processing power and scope. The impact of botnets on ransomware is evident when examining the Russian ransomware *CryptoLocker*. Released in September 2013, *CryptoLocker* was the brainchild of Russian cybercriminals, including the Russian cybercriminal and mastermind of the botnet "*GameOver Zeus*", Evgeniy Mikhailovich Bogachev (The United States Department of Justice, 2014) and focused on targets based in North America and Western Europe (Jarvis, 2013).

Infecting a quarter of a million computers globally before the end of 2013 (Blue, 2013), *CryptoLocker* was a revolutionary type of ransomware that would illustrate ransomware's business potential (CrowdStrike, 2021b).

CryptoLocker employed a tactic not seen in previous ransomware versions, using the peer-to-peer botnet *GameOver Zeus* to further distribute the malware (O'Kane et al., 2018; Ward, 2014). Using botnets to spread the program, *CryptoLocker* became a highly effective form of ransomware that could be readily propagated to thousands of devices with little effort from the creators. Arguably, *CryptoLocker's* ability to increase the scope of their cybercrimes would play a significant role in not only the development of Russian ransomware but would influence the appeal of ransomware to Russian organised cybercrime groups. Botnets provided Russian cybercriminals with the ability to conduct their ransomware activities on a considerably larger scale than early ransomware such as *AIDS Trojan*. *CryptoLocker* would extort roughly USD$3 million in the eight months their program was active before its takedown in June 2014 (O'Kane et al., 2018), significantly more than that of the *AIDS Trojan*, which ultimately resulted in no profits for the creator.

Furthermore, the introduction of botnets can be correlated to the future growth of Russian RaaS as it would provoke a change in how Russian cybercriminals conduct their illicit activities. Botnets highlighted to Russian ransomware groups that their new technological capabilities provided them with additional profit channels beyond ransomware alone, including cyber espionage, large-scale data exfiltration and extortion (Bederna and Szadeczky, 2019). The combination of new technology and the cybercrime skills that existed within Russia provided the perfect environment for the growth of ransomware like CryptoLocker.

Additionally, due to the increased scalability provided by botnets, Russian organised cybercrime groups could take their operations from just "one-off events" and instead expand their operations to an industrial scale (House of Representatives Standing Committee on Communications, 2010), generating significantly larger profits than previous ransomware programs including *AIDS Trojan*. Homayoun et al. (2018) expand on this argument and highlight how botnets enabled operations to increase due to the ability of bot malware to constantly advance and circumvent any existing

measures that may have been put in place to protect a system from ransomware. Furthermore, botnets enabled Russian organised cybercrime groups to create an additional revenue stream beyond ransomware through the commodification of ransomware botnets (Steadman, 2012). Grabosky (2016) highlights that the commercialisation of hacker tools has been more commonplace over the last two decades, with botnets including *GameOver Zeus* readily available for sale or rent online; this commercialisation of the hacker landscape has provided cybercriminals with an additional and low-effort way to generate profits.

A subsequent influence on the growth of ransomware in Russia was the introduction of ransomware with tailorable code, as seen in the rise of *CryptoWall*. While previous versions of ransomware programs had code that could not be altered extensively by the users, *CryptoWall's* programming allowed cybercriminals to tailor the ransom demand and the victim's country of origin. Mimicking the methodology and appearance of *CryptoLocker*, *CryptoWall* continued to target Microsoft-based machines and spread its code through malicious emails (Hassan, 2019). *CryptoWall* did, however, differ from its predecessor in several ways, which made it an appealing program to Russian organised cybercrime groups. While *CryptoLocker* became obsolete once its code was isolated, and the encryption key was recovered, CryptoWall has remained prevalent within the cyber landscape due to its proclivity to evolve due to the ransomwares' adaptive programming, which included an isolated encryption key (KnowBe4, 2022).

The *CryptoWall* program has undergone several variations since its creation in 2014 (Hassan, 2019; Zaharia, 2022). These variations allowed the cybercriminals behind the program to fix errors or weaknesses in previous version codes, such as implementing "self-protection mechanisms" (Mohanta et al., 2018). This self-protection was achievable due to cybercriminals developing new techniques and technology that would protect the ransomware, including creating programs that could conceal itself within a system or obstruct the functionality of a device's antivirus or firewall (Shevchenko, 2007). Moreover, the flexibility within the *CryptoWall's* program provided by its tailorable code would bolster the appeal of ransomware to Russian-based cybercriminals as it suited the flexibility within

Russian crime groups and allowed the groups to evade law enforcement both in Russia and globally.

However, the most distinguishing feature of *CryptoWall* that made it so appealing to Russian cybercrime groups lies within its code. *CryptoWall's* code contains specific instructions for the malware to not infect machines within countries picked by the program's creators. In the case of *CryptoWall*, machines located in Russia, Ukraine, Kazakhstan and Belarus were safe from the program's destruction (Cyber Threat Alliance, 2018; Mohanta et al., 2018). While it has been established that there was always some level of dictating who would fall victim to a ransomware attack, formulating the parameters of an attack was time-consuming and led to slow and limited results, as seen in the *AIDS Trojan* (O'Kane et al., 2017; Ryan, 2021). *CryptoWall's* tailorable code bolstered its appeal to Russian cybercriminals, evidenced by the almost twenty thousand Australians falling victim in 2014 (Karlovsky, 2014) and the USD$18 million profits that would be generated in just a year (Fisher, 2015). Remarkably, it would be the ability to tailor ransomware code that would later contribute to the shift in the Russian state's role within the ransomware landscape and the cultivation of RaaS, as tailorable code would enable the Russian state to direct attack on specific enemies of the Kremlin.

CryptoWall paved the way for the broader appeal of ransomware to cybercriminals by allowing them to tailor their code to attack only specific victims. Specifically, *CryptoWall* provided Russia-organised cybercrime groups with the ability to avoid targeting Russia and Eastern European nations, which provided additional protection from potential prosecution by Russian authorities. Ortner (2015) and Krebs (2021d) expand on this argument, highlighting that due to a lack of due diligence regarding the protection and prosecution of transnational cybercrimes, Russian organised cybercrime groups could tailor their ransomware code to only target victims from predominantly Western nations to avoid negative ramifications since Russian rarely extradited cybercriminals to Western nations (Canales, 2021). With the possibility of conducting criminal activities with little to no consequences while still making hundreds of millions of dollars (O'Kane et al., 2018), ransomware like CrytoWall made the malware even more appealing to Russian cybercrime groups.

Notably, the ability to tailor ransomware programs to attack or avoid specific targets would become an appealing prospect to cybercriminals during the Annexation of Crimea in early 2014. While the large-scale use of ransomware was not utilised in the initial stages of the Crimean conflict, at least not until *NotPetya* in 2017, cybercriminals did use their ability to tailor ransomware to attack Ukrainian targets as a form of patriotic cybercrime activity. Evidence of the appeal of tailorable code to patriotic Russian cybercriminals is seen during the attack of a Ukrainian power grid in late 2015 (Zetter, 2016) by the Russian military hacker group *Sandworm* (Greenberg, 2019). The attack underscored cybercriminals' ability to target specific organisations and how sophisticated and destructive ransomware could be (Greenberg, 2019). Most notably, while the Russian state did not actively sponsor ransomware threat actors during this time, the state was a soft benefactor of cybercriminals attacking Ukrainian organisations.

The final influence on the rapid growth of Russian-based ransomware came in the form of cryptocurrencies, in particular Bitcoin. Deployed by Satoshi Nakamoto in 2009 (Kethineni et al., 2018), Bitcoin is a blockchain-based decentralised, peer-to-peer networked currency that circumvents the necessity for traditional banking (Conti et al., 2018a; Conti et al., 2018b; Introna and Pecis, 2019). The introduction of cryptocurrencies within the cyber landscape allowed cybercriminals, including Russian ransomware groups, to manipulate this new technology to improve their existing criminal activities (Kethineni et al., 2018) and circumvent the restrictions that existed using traditional banking methods. In the case of ransomware, it allowed Russian cybercrime groups to anonymise their activities further.

While previous versions of ransomware either demanded payment via wire transfer or alternative payment services such as PayPal (Higbee, 2018; O'Kane et al., 2018), *CryptoLocker*, and *CryptoWall* were the first to demand payment via Bitcoin (Mohanta et al., 2018). With cryptocurrencies, Russian cybercriminals could now demand ransom payments without involving third-party financial institutions or alternative money transfer organisations (Higbee, 2018; Kethineni et al., 2018). Additionally, when payment was received, cybercriminals could utilise a tumbler or mixer to obscure further the link between the cryptocurrency and their wallet or address (Buil-Gil and Saldana-Taboada, 202; Kethineni et al., 2018).

Similar to the appeal created by tailorable code, the introduction of cryptocurrencies like Bitcoin undeniably contributed to the rise in Russian-based ransomware as it provided a further level of protection to organised cybercrime groups to conduct their activities with an increased level of security. Bitcoin and other cryptocurrencies have reduced the effectiveness of law enforcement in effectively conducting ransomware investigations (Choi, 2015; Lee and Choi, 2021). Additionally, Bitcoin allowed the ransomware process to be streamlined due to the exclusion of traditional financial institutions, making the crime significantly more coinvent for crime groups (Braaten and Vaugh, 2021). A concept that has been explored extensively, with Gottschalk (2017a; 2017b) arguing that the offenders will turn to convenient and more time-efficient criminal methods if it results in a greater potential for future profits.

To expand on this argument, CrowdStrike (2021b) highlights that the introduction of easily accessible cryptocurrency exchanges such as Coinbase and Binance provided cyber criminals with the ability to receive their anonymous ransoms almost instantly. However, it was the growth in unregulated cryptocurrency exchanges that aided ransomware groups in truly made cryptocurrency more accessible. Unlike regulated exchanges that require customer identification and maintain anti-money laundering policies, unregulated exchanges offer anonymous trading and limited regulation (Alexander and Heck, 2020). Furthermore, the utilisation of cryptocurrency and crypto exchanges provided ransomware groups with the ability to circumvent some of the sanctions placed upon Russia during the Crimean conflict, providing groups with the ability to circumvent economic restrictions (Davies, 2019). Arguably, the introduction of cryptocurrencies provided cybercriminals with a level of financial freedom not available previously. The addition of cryptocurrencies within the ransomware landscape undeniably made the malware an even more appealing form of cybercrime for Russian organised crime groups and played a key role in the evolution and growth of ransomware.

The increased accessibility to botnets, the ability to tailor ransomware code and the introduction of cryptocurrencies significantly increased the appeal of ransomware and would contribute to the eventual rise in Russian RaaS. However, while *CryptoLocker* and *CryptoWall* were both Russian-based ransomware programs that

contributed significantly to the growth of ransomware in Russia and paved the way for the next generation, the worst forms of Russian ransomware were yet to come.

2.2 The Rapid Expansion of Ransomware

Following *CryptoLocker* and *CryptoWall*, three ransomware programs contributed to the rapid expansion of ransomware by Russian cybercrime groups and the eventual rise of Russian RaaS; *WannaCry*, *NotPetya*, and *DarkSide*. *NotPayta*, *WannaCry* and *DarkSide* were all ransomware variants that, while initially appearing to be updated versions of previous malware, performed differently from the standard ransomware of the past due to three features: the active involvement of the Russian state within the ransomware landscape, the scale, and the precision of the programs. During this rapid expansion, Russia organised crime, and the Russian state would move closer to RaaS due to the new disruptive possibilities that ransomware provided.

2.2.1 The Russian Government's NotPetya

While resembling code from a previous ransomware program, *Petya*, which circulated in 2016 (Greenberg, 2019), *NotPetya* was a whole new beast that, during its peak in 2017, crippled multiple organisation's systems, including those within Ukraine, France, the United Kingdom, and the United States (Greenberg, 2019). NotPetya represents a key player in the expansion of ransomware due to the proposed motivations behind its creation, which would play a role in the eventual growth of Russian RaaS. *NotPetya* differed from previous versions of Russian ransomware in two notable ways: it was created not by Russian cybercriminals but by *Sandworm* (Greenberg, 2019), highlighting the shift in the Russian state becoming an active player within the ransomware landscape, and unlike previous versions of ransomware, *NotPetya* did not offer to decrypt files following the ransomware payment. Instead, *NotPetya*, due to its code, utilised a "scorched earth" corruption method that meant that the cybercriminals could not provide any decryption keys to victims to gain back access to their data (Greenberg, 2019; Zorz, 2017). The lack of a decryption key made *NotPetya* such a damaging ransomware program; unlike previous ransomware programs where profit was the primary

motivation, *NotPetya* only sought to destroy data and sabotage those systems attacked (Greenberg, 2019; Hassan, 2019).

NotPetya, like *CryptoWall*, emphasised how cybercriminals could utilise ransomware as a targeted cyber tool. Greenberg (2018) proposed that *NotPetya* was a program designed by Russian military hackers as a "weapon" against Ukraine-based infrastructure that established a precedent of nation-states utilising ransomware to destroy an enemy's computers. Furthermore, the use of ransomware by the Russian government highlighted to organised crime groups not only the potential for ransomware as a tool for financial gain but underscored the legitimacy of ransomware as a tool to gain power. The impact of *NotPetya* and Russian state-sponsored cybercrime will be analysed further in chapter three; however, NotPetya would be the first instance of the Russian state becoming actively involved within ransomware by conducting attacks themselves, in contrast to their soft benefactor position during previous ransomware programs. Furthermore, *NotPetya* would also demonstrate to Russian organised cybercrime groups the destructive and powerful nature of ransomware, which would contribute to the rise of RaaS in Russia.

2.2.2 WannaCry and the Increased Scale of Ransomware

The next program that influenced the expansion of ransomware would also occur in 2017, with the appearance of *WannaCry*. *WannaCry* is evidently not a Russian-based ransomware program but a creation of the North Korean government (The United States Department of Justice, 2018); however, the program's scale and notoriety significantly impacted the landscape and, like *NotPetya*, highlighted the appeal of ransomware to organised cybercrime groups. While some academics argue that *WannaCry* was nothing new within the ransomware landscape in terms of deployment methods, code and payloads (O'Kane et al., 2018) and that its creators were careless with the program's code (Greenberg, 2019), the significance of WannaCry cannot be downplayed. Infecting over 300,000 computers in over 150 countries, including the National Health Service (NHS), in just a day (Department of Homeland Security, 2017; Turner et al., 2019), *WannaCry* played a critical role in the adoption of ransomware by organised crime groups due to its scale (Baldwin and Dehghantanha, 2018; Turner et al., 2019).

While arguably there were design flaws within *WannaCry*, and the Return on Investment (ROI) was small in comparison to other programs such as *CryptoWall* (Greenberg, 2018; Turner et al., 2019), *WannaCry* was a highly effective form of ransomware as its code was able to propagate globally in a concise timeframe (Turner et al., 2019). Through this dramatic infection rate, *WannaCry* had a substantial impact on hardware and resources (The United States Department of Justice, 2018) and resulted in patient harm and the loss of life when the effects on the NHS and German Hospitals are accounted for (Ghafur et al., 2019; Westman, 2020). Unlike any previous version of ransomware, *WannaCry* was the first to have physical world implications that resulted in death. *WannaCry* highlighted to Russian organised cybercrime groups the true potential of ransomware as a business that could be both scalable and profitable. While *WannaCry* only resulted in a revenue of 52 Bitcoin, roughly USD$143,000 at the time, the potential of ransomware was once again made apparent.

WannaCry's attack on organisations, including the NHS, highlighted to Russian organised crime groups the financial potential of using ransomware against specific vulnerable sectors where their attacks would be felt most. Sectors with historically weak security, including health, education, and infrastructure, are prime targets for ransomware due to their vulnerabilities and valuable data (Coker, 2022). *WannaCry* highlighted to Russian ransomware groups the weakest industries and the potential profits that could be collected from them. Overall, while not a Russian-based ransomware program, *WannaCry* highlighted to Russian cybercriminals the capacity of ransomware to infect and extort money on an enormous scale.

2.2.3 The Precision and Dread of DarkSide

The final ransomware to make the most significant impact on the adoption of ransomware by Russian organised crime groups was the Russian-based program *DarkSide*. Named after the cybercrime group that created the program, also known as *Carbon Spider*, *DarkSide's* claim to infamy was during their attack on the American oil pipeline system Colonial Pipeline in May 2021 (Reeder and Hall, 2021). *DarkSide* attacks Windows and Linux-based systems that failed to patch a vulnerability within the virtual machine VMware ESXi (CrowdStrike, 2021c) and targets large companies within several industries other than healthcare, education

and the government (Falco, 2022; Krebs, 2021b). *DarkSide's* scale is considerably smaller than previous ransomware programs, with only ninety victims reported in mid-2021 (Trend Micro Research, 2021b); however, *DarkSide* reportedly obtained over USD 90 million from just forty-seven of those victims (Sharma, 2021). Even with its smaller scale, *DarkSide* has caused a significant threat to critical infrastructure organisations (Australian Cyber Security Centre, 2022b).

DarkSide led the way in the ransomware landscape by utilising double extortion to ensure profits (Cybereason, 2021). The technique involves exfiltrating the victims' data before encryption and demanding a ransom payment to decrypt the data and prevent the data from being sold on the dark web (Kerns et al., 2022). This extra level of extortion set *DarkSide* out from previous versions of ransomware, including *CryptoLocker* and *CryptoWall*, as it provided cybercriminals further assurance that they would gain profit from their ransomware activities. While this feature of *DarkSide* played a crucial role in contributing to the financial appeal of ransomware and the eventual rise of RaaS, it is not this feature that contributed to the overall appeal of ransomware to Russian organised cybercrime groups.

Instead, the significance of *DarkSide* lies in the level of panic it created during the Colonial Pipeline attack. *DarkSide* resulted in the shutdown of the pipeline for a total of ten days, resulting in panic buying from consumers, social disruption and impacts on U.S. fuel delivery (Falco, 2022; Reeder and Hall, 2021). The panic created by *DarkSide* is where its importance lies; while Gomez (2021) questions the power that panic or "cyber doom" holds in influencing the public, they do not consider the impact panic creates beyond cyberspace. *DarkSide* during the Colonial Pipeline had the power to influence society beyond the cyber landscape, causing both broader economic impacts in the form of higher gas prices and anxious consumers (Romo, 2021). Through its massive profits of USD$90 million in Bitcoin, *DarkSide* highlighted to Russian cybercriminals the ability of ransomware to produce massive profits when fear and panic are exploited.

NotPetya, *WannaCry*, and *DarkSide* were significant steps in the evolution of ransomware. They demonstrated to Russian organised cybercrime groups and the Russian government that ransomware was not just another form of cybercrime but a

cybercrime that could generate considerable profits and harm due to its dramatic and large-scale impacts. However, while these programs would play a key role in the adoption of ransomware by Russian organised crime groups, RaaS would demonstrate to Russian cybercriminals and the Russian state the potential of ransomware.

2.3 The RaaS Business

2.3.1 RaaS Overview

Arguably, just as ransomware was not a new concept within the cyber landscape, the same can be said for RaaS. Cybercriminals have been offering their skills on the dark web for several years (Liska and Gallo, 2019). However, RaaS provides a new world of possibilities for those that lack the knowledge or infrastructure to become active and dangerous threat actors (Meland et al., 2020), providing affiliates with the ability to execute pre-developed ransomware tools and earn a percentage of the profits with limited hacking skills. With RaaS groups receiving over USD$600 million in profits in 2021 (Paganini, 2022), the threat of the RaaS business cannot be understated.

RaaS provides those with the skills to conduct cybercrime activities with an opportunity to generate profits by selling their services (Meland et al., 2020; O'Kane et al., 2018). RaaS differed from previous ransomware programs as it allowed organised cybercrime groups to expand their operation beyond just extorting individuals and organisations with one program. Instead, RaaS provided various options and models that made it much more appealing to Russian cybercriminals. RaaS is not one sole model; rather four standard RaaS models are utilised by organised cybercrime groups. These models include monthly subscriptions, affiliate programs, a one-time license fee, and profit-sharing (Baker, 2022). The service offerings also vary from group to group, with some groups offering customisable versions of ransomware and others providing fully functioning exploit kits that include ransomware within the package (Liska and Gallo, 2019).

The role of the RaaS groups within their role as the operator is to recruit

affiliates to their service, provide affiliates with a ransomware package that includes the malware and a "command and control" dashboard, organise the victim payment portal and assist with any victim negotiations (Baker, 2022). Depending on which RaaS group is involved, they may also assist the associate with managing stolen information, as seen with the RaaS group REvil and their "Happy Blog" (Baker, 2022). With their different models and offerings, the overall goal of these RaaS groups is to stand out from the competing groups and appeal to the largest number of affiliates. RaaS has become a highly appealing form of cybercrime for Russian organised crime groups through the simple option of providing them with the ability to expand their operations and tailor and market their criminal services.

2.3.2 The Ransomware Business and the Russian State

The significant shift that contributed to the growth of ransomware and the adoption of RaaS by Russian organised crime groups lies in the shift of ransomware into a lucrative and highly organised criminal business (O'Kane et al., 2018). The business-like improvements made to ransomware by Russian organised crime groups are diverse; however, two key influences contributed to the shift of ransomware to a business model; profit and power. To increase profits, Russian ransomware groups adapted the existing ransomware and shifted their targets, adopted new methods of ransom extortion and created new recruitment tactics that would bring in highly skilled individuals into Russian ransomware groups. To increase power, Russian ransomware groups turned to RaaS as a tool that could be used to benefit and support the Russian state, which in turn would support their desire for control.

Historically, ransomware attacks were a numbers game with cybercriminals attempting to accumulate as many victims as possible to obtain maximum profits (Meland et al., 2020; Symantec, 2019). In contrast, RaaS, due to its shift to a business model, focuses more on lucrative targets or Big Game Hunting (BGH) to produce revenue (CrowdStrike, 2021a). Cybercriminals have sought to improve their skills and the complexity of their programs to ensure higher success rates. Ransomware groups were now mimicking the capitalistic mentalities of everyday companies. Evidence of these improvements is apparent when comparing the payouts of RaaS groups compared to earlier ransomware attacks. For example, CryptoLocker made close to USD$520,000 from 944 addresses (Hassan, 2019),

whereas DarkSide made USD$4.4 million from the Colonial Pipeline attack alone (Reeder and Hall, 2021). The shift by RaaS to BGH correlates with organised cybercrimes' desire for power as it coincides with the desires of the Russian state. Primarily from Western nations, the disruption of BGH organisation's directly benefits the Russian state as some of the profits are funnelled to the Kremlin (Davidson, 2022), all while bolstering the perceived power of the state. Through their active support of the Kremlin, RaaS groups are provided with a level of control and freedom by the Russian state.

The shift of ransomware to a business model resulted in significant profits for crime groups and changed how organised crime groups would extort ransomware from their victims. RaaS and the focus on ransomware as a modern business saw the rise of double and triple extortion (Cybereason, 2021; Snowden, 2021). RaaS group's sole motivation is to generate profit, which depending on the model utilised, relies predominantly on the payment of the ransom. Therefore, Russian ransomware groups have looked to new methods to obtain payment.

The ever-increasing need for profits has inevitably resulted in the rise in double and triple extortion models. The double extortion method has been employed by the majority of RaaS groups, including the above-mentioned DarkSide and *REvil*, who use their dark web blogs to share data from stolen organisations (Baker, 2022; Cybereason, 2021) along with *NetWalker* (Krebs, 2021a) and *DoppelPaymer/Indrik Spider* (Unit 42, 2021). The RaaS group *BlackCat* (also known as *ALPHV*) has utilised triple extortion since its unearthing in November 2021. Like double extortion, the group demands payment to decrypt the data and prevent stolen data from being released to the public; however, they go a step further and threaten to DDoS the victim's system if the ransom is not paid (Avertium, 2022; Kerns et al., 2022).

As the number of RaaS groups rises and their monetary motivation increase, these groups will likely look to additional levels of extortion, with quadruple extortion that involves the harassment of an organisation's clients (Vaas, 2021) to likely be the new normal. However, while groups may continue adding additional layers of extortion, Cusack and Ward (2018) argue that RaaS groups will find their crime models economically unfeasible and will fail over time. The hyper-focus on profits and the

growth in extortion methods make RaaS an even more alarming threat to government and organisations as it only increases the difficulties in defending against RaaS groups. Additionally, as the appeal of profits generated through these multi-layer extortions increases, the rise of RaaS and Russian ransomware groups could potentially increase. The increased level of extortion coincides with the additional involvement of the Russian state within RaaS. Data gathered during the extortion process, while being primarily utilised for profit, is also a tool used by RaaS to gain support from the Kremlin, with information potentially being shared with Russian intelligence (Weber, 2022). Through sharing valuable information and developing a beneficial relationship, RaaS groups can gain further control within Russia, and the Kremlin can maintain its power over the state.

The shift of ransomware as a business has contributed to a shift in the ransomware recruitment culture and, in turn, increased the popularity of RaaS to Russian organised crime groups. As the number of RaaS groups has grown, so has the appeal of joining these groups. While early ransomware programs were created and executed by individuals, such as Zain Qaiser (Casciani, 2019) and Evgeniy Mikhailovich Bogachev (Mohanta et al., 2018), RaaS groups with their business-focused mentalities are instead openly recruiting skilled hackers into their groups. Within dark web forums, RaaS groups such as *BlackCat* actively recruit new members, with their focus on ex-members of other RaaS groups such as *REvil*, *DarkSide* and *BlackMatter* (Hill, 2022) but also members of the hacker and organised crime forums (Meland et al., 2020; Wall, 2021).

Adopting these new recruitment tactics and turning ransomware into a business, ransomware groups are again mirroring the tactics of legitimate information technology businesses that bring in the best and brightest into their ranks to increase their profits. Additionally, the shift in recruitment reflects that of the tactics utilised by the Russian state, with the FSB historically recruiting cybercriminals to act as “patriotic hackers” (Lokot, 2017) on behalf of the Kremlin. The mirror of Kremlin recruitment further highlights the desire by RaaS groups for power and support from the Russian state as it underlines their need for a direct connection to the Kremlin and the elite within Russia.

Shapiro (2021) expands further on the change in ransomware recruitment and argues that the rise of cybercrime, including the dramatic growth in the scale of RaaS groups, has contributed partly to the development of the crime gig economy. Just as the legitimate gig economy provides independent workers with the opportunity for profit, the crime gig economy created a market system where desperate individuals are given the ability to increase their financial prospects through untethered and informal illicit ventures (Shapiro, 2021). Through outsourcing their skills, cybercriminals have utilised RaaS to generate a profit during situations where abundant financial opportunities are limited. Likewise, the growth of RaaS and the gig economy have made partnering with new RaaS groups appealing and potentially more financially viable than acting as a lone wolf.

Although notably, the active recruitment of new skilled hackers may be a charade, and hackers are merely moving from their original RaaS to a reinvented version as a ploy to hide their members and provide a renewed level of security; as seen in the *Ryuk* RaaS group's potential renaming to *Conti* in 2020 (Australian Cyber Security Centre, 2022a; Krebs, 2021c). Once again RaaS group have mirrored the tactics of the Russian state in a bid to maintain power. Notably, the Kremlin has historically recruited hackers from the criminal underworld and cycled them through government organisations, including the FSB and the Russian military (Kramer, 2016). Through the continual rotation of patriotic hackers, the Kremlin has found a way to conduct their special cybercrime operations with an additional layer of anonymity for their hackers. Overall, the shift in RaaS recruiting and the mirroring of Kremlin techniques exemplifies that ransomware, as it has evolved, has become a genuine criminal enterprise compared to where it began in 1989.

This chapter explored the evolution of Russian ransomware and the growth of RaaS. It examined the broader aspects of ransomware's evolution that have contributed to the growth of Russian RaaS. Particularly, the development of new technologies, the ongoing influence of the state within the ransomware landscape, an increase in scalability and level of harm, and the rise of more accurate programs. The prominence of ransomware within Russia highlights the ongoing connection between Russia, organised cybercrime, and the state. The next chapter will look in detail at

the evolution of Russian organised crime toward RaaS and the role of the political-criminal nexus within this evolution.

Russian Organised Crime and the State

Russian organised crime has a long and complex history that even predates aspects of the American Cosa Nostra (Reuter and Paoli, 2020). While organised crime groups can be traced back to the 1700s Russia (Varese, 2001), the Bolshevik Revolution saw the growth of the most notable criminal network that would create the foundation of what would become the sophisticated RaaS groups of today, the *vory v zakone* (Thieves in Law). While the criminal ideals and the “network of strict regulations” (Varese, 1998: pp. 515) ingrained in the *vory v zakone* are notable characteristics that have contributed to the enduring strength of Russian organised crime, the most significant factor that has influenced their survival is the relationship

between organised crime and the Russian state. Through changes in culture, technology, the introduction of globalisation and new political powers, Russian organised crime has shifted and mutated (Galeotti, 2018b); however, the relationship between organised crime and the state has been preserved.

Current literature on Russian organised crime has effectively highlighted the characteristics of traditional and modern Russian organised groups, with Galeotti (1998, 2004, 2017, 2018a, 2018b) providing extensive insight into the history of the *vory v zakone* and their modern iterations. However, while previous research, including Galeotti's, provide insight into the inner workings of Russian organised crime, there is a significant gap regarding the evolution of Russian organised crime towards RaaS and the influence of the Russian state on this evolution. This chapter examines this gap within the literature and explores the history of Russian organised crime and the notable aspects of its evolution. Furthermore, this chapter analyses the factors that have contributed to the evolution of Russian organised crime towards RaaS, primarily the role of the political-criminal nexus and socio-technological impacts in influencing the evolution toward RaaS. While previous literature has provided a great deal of insight into the workings of Russian organised crime, this chapter builds upon the work of Galeotti and other noteworthy scholars by examining the external factors that have contributed to the evolution of traditional and modern Russian organised crime groups and the continual influence of the Russian state on this development.

3.1 Political-Criminal Nexus

Before examining the evolution of Russian organised crime towards RaaS, it is essential to explore the leading factor that heavily influenced that evolution; the political-criminal nexus. The political-criminal nexus is the active partnership between individuals at the highest levels of government to the lowest level criminal (Hughes and Denisova, 2001). The relationship between the political and criminal world is a chronic issue that undermines a state's law and economic development as organised crime groups gain control over crucial areas of society (Godson, 2003). While the reasons for establishing the nexus vary, the goals are simple; power and money (Hughes and Denisova, 2001). These goals have tightly bound Russian organised

crime groups to the elite that wish to hold onto their kleptocratic control, highlighting the inseparability of the Russian state to organised crime.

While the nexus exists in many countries, Russia became the perfect breeding ground for the political-criminal nexus due to the unstable political and economic conditions (Godson, 2003). Shelley (2003) argues that while the nexus existed in the Soviet era, the fall of the USSR would provide the perfect environment for the political-criminal relationship to flourish due to the push for privatisation, economic instability within the state and the symbiotic bond between the political establishment and the criminal underworld. Furthermore, Galeotti (2017) proposed that institutionalised corruption that existed even before the fall of the USSR would only aid in blurring the lines between the criminal 'underworld' and the political 'upperworld', solidifying the political-criminal nexus.

Throughout the history of Russian organised crime, the political-criminal nexus has continuously evolved, strengthening to become more ingrained within the political landscape. While previous research has examined the symbiotic relationship between the Russian government and organised crime during the Soviet Union and the early years of the Russian Federation, there is a notable gap in how the political-criminal nexus has explicitly evolved and how that evolution has influenced the decisions of Russian organised crime groups. This section aims to build on the previous research and utilise the political-criminal nexus to analyse the evolution of Russian organised crime toward RaaS. Through examining organised crime's evolution through the lens of the political-criminal nexus, a more holistic understanding of the role of the Russian state within RaaS is possible as the inseparable nature of the state and the criminal underworld becomes apparent.

3.2 Traditional Russian Organised Crime

3.2.1 Vory v Zakone and Stalin

Galeotti (2018b) put it succinctly when he states that traditional Russian organised crime groups were moulded by the actions of three leaders; Stalin created the "collaborator-criminal" (pp:81), Brezhnev created the black markets, and finally, Gorbachev created the new markets. While the foundation of traditional organised

crime groups began with the horse thieves and the criminal subcultures of the pre-Soviet era (Galeotti, 2018b; Shearer, 1998), the pinnacle of traditional crime groups began in the era of Stalin as the *vory v zakone*. Forged within Stalin's gulags from 1922 to 1952, the criminals that would make up the *vory* were seen as equally parasitic to socialism as the capitalist was (Lenin, 1915 as cited in Galeotti, 2018b). Through their interactions within the gulag system, these criminals would become more connected and eventually form a secret criminal society comprising its own code of conduct and rituals (Varese, 1998).

During their time in the gulags, the *vory v zakone* would collaborate not solely to conduct criminal activity within the camp but rather to acquire leadership roles and prevent work from being conducted (Varese, 1998). A key point to consider is that the *vory* used their power and influence to benefit those within the brotherhood rather than influence politics or society. Galeotti (2018b) indicates that the *vory* would use their power to bribe officials within the gulags to ensure that they could continue their business; this was done using the *vory's obschchak* fund, a communal fund collected by prison inmates. The *vory's* code strongly dictated the acceptable crimes for members to commit; for example, the *vory v zakone's* code was firmly against violence, and members were to conduct their criminal activity without bloodshed (Varese, 1998). However, the true scope of this rule is debated; Vincent (2020) disputes Varese's (1998) claim and argues that violence was often used by the *vory* to gain respect and power within the *vor*.

While the *vory v zakone* held considerable power and wealth within the gulags, they did not exude control over the broader society as seen in other mafias such as Cosa Nostra or 'Ndrangheta (Paoli and Reuter, 2020). Furthermore, the *vory v zakone* had not yet formed their critical relationship with the political elite. While the political-criminal nexus did not exist during the Stalin era, the early years of *vory v zakone* did see the foundations of this relationship form, with the "collaborator-criminal" forming relationships with the elites within the prison system. The *vory v zakone* during the Stalin era would conduct activities that would foster their control of the prisons; this desire for control would create the foundation for the motivators behind Russian organised crime, forming their nexus with the political elite. However, like all organised crime groups, *the vory v zakone* would adapt and soon shift away from the

gulags and towards the profit-motivated criminal enterprise with influence over the socio-political landscape, all from the decisions of Leonid Brezhnev.

3.2.2 Brezhnev and the Secondary Economy

Following the death of Joseph Stalin, Leonid Brezhnev took the office of Secretary of the Communist Party of the Soviet Union from 1964 until 1982. Under Brezhnev, traditional Russian organised crime groups, including the *vory v zakone*, shifted their focus from controlling their members and the communal *obschchak* fund to building a profit-focused operation. While the *vory* still emphasised theft as a fundamental crime pillar, they also focused on extortion and cons to gain a profit (Albini et al., 1995: pp. 217). This trend would continue throughout the evolution of Russian organised crime and still ring true for organised RaaS groups. The catalyst for this change in motivation resulted from the Communist Party of the Soviet Union primarily focusing their investment on military spending rather than social spending, along with rampant corruption within the Communist Party and Russian society (Galeotti, 2018b). Vaksberg (1991) argues that this shift occurred due to the "political gangsterism" (pp. 19) approach adopted by Brezhnev as he and the political elite strove for power. A by-product of these failures within Brezhnev's Russia was organised crimes shift to criminal activities that would fill the gaps in official markets; the *vory* began focusing on bribery, black markets, and *blat* – the exchange of favours (Albini et al., 1995; Galeotti, 2018b).

Brezhnev's period in power highlights the influence of socioeconomics on Russian organised crime. Previous research has argued that the socioeconomic landscape heavily influences not only the rise in crime but also the number of individuals turning to organised crime as a method to lift themselves from potential destitution (Bourguignon, 1999; Mauro and Carmeci, 2007; Siegel, 2012). Specifically, that high unemployment, low economic growth, and political corruption strongly influence individuals turning to organised crime (Mauro and Carmeci, 2007). Albini et al. (1995) expand on the connection between socioeconomics and organised crime in Russia, highlighting organised crime's manipulation of the socioeconomic landscape within Russia to their advantage, most notably the corruption that resulted from the low economic growth within the state. For example, the *vory* manipulated the prevalent corruption at the time and developed close ties with corrupt Party officials

and *tsekhoviki* – owners of black-market factories. Utilising opportunities provided by the black markets to take not only a cut of the earnings but also occasions to flex their power during disputes within the criminal underground (Cheloukhine, 2008; Galeotti, 2018b). The development of close ties between Russian organised crime and Party officials would mark the beginning of a long-standing nexus between the two groups.

As a result of the socioeconomic landscape during the Brezhnev era, Russian organised crime sought to strengthen their relationship within the state to expand their control within the broader Russian society. Instances of bribery of public officials increased, and the rise of criminal crony politics within the Russian political landscape was solidified (Shelley, 2003). The Brezhnev era emphasised the significant impact a weak state can have on the political-criminal nexus (Shelley, 2003) and validated the role of organised crime in shaping the political landscape (Briscoe and Kalkman, 2016). While the seed of corruption and the political-criminal nexus was planted during Stalin's era, Brezhnev's failings would fertilise the seed. However, while Brezhnev's time in power would result in significant changes in the motivations and partnerships of Russian organised crime, the most substantial change would not occur until the late 1980s and early 1990s.

3.2.3 Gorbachev's Liberal Reforms

The most significant change to traditional Russian organised crime would be seen in the final years of Mikhail Gorbachev's time as the General Secretary of the Communist Party, which ended with the fall of the USSR in 1991. The decisions made during Gorbachev's time in power would not only contribute to the growth of organised crime's control and the strengthening of the political-criminal nexus but would see the rise of newly established organised crime groups (Glenny, 2008). Gorbachev's *perestroika* reforms, such as *Glasnost*, aimed to liberalise the economy; however, these reforms, such as the opening of the economy to cooperatives and delegitimisation of the Communist Party (Galeotti, 2018b), would only provide Russian organised crime with new victims and criminal opportunities (Albini et al., 1995; Galeotti, 2018b). As those in power attempted to hold onto whatever control they could following these reforms, Russian organised crime would manipulate the political elites to form relationships that would benefit both groups.

Due to these rapid societal changes (Albini et al., 1995), crime groups shifted away from solely profit and instead had the overarching goal of power (Nikforov, 1993, Shelley, 1995).

Gorbachev's policies aimed to open the Russian economy to new private enterprises would allow organised crime groups to launder and reinvest their funds through vulnerable entrepreneurs (Albini et al., 1995; Galeotti, 2018b; Glenny, 2008; Tomass, 1998). Protection rackets such as those seen previously in the Italian American Cosa Nostra became the new flavour for Russian organised crime (Albini et al., 1995; Nikforov, 1993). In 1989, seventy-five per cent of these private enterprises were controlled by organised crime groups (Galeotti, 2018b), emphasising the scale of Russian organised crime's power at this point. With their hold on Russian private enterprises in place, it is during this time that the line between Russian organised crime and the state begins to blur. The institutional relationships established during the Brezhnev era were now perfectly positioned to ensure that organised crime groups could use their political connections to conduct their business without interruption (Xiao, 2016), with the political elite and organised crime benefitting from the increase in power and profit that their relationship provided.

3.2.4 Post-Soviet Organised Crime

Following the collapse of the Soviet Union in the latter half of 1991, Russian organised crime experienced a notable shift in its motivations, structures and behaviours that would have continuing impacts in the following decades. The hierarchical structure that was present in many of the traditional organised crime groups (Pace and Style, 1975; Paoli and Reuter, 2020) was gone, and in its place were flexible networks of "semi-autonomous criminal entrepreneurs" (Galeotti, 2004: pp. 55). Due to this flexible structure, Russian crime groups of the 1990s and early 2000s turned their focus away from crimes such as drug smuggling and prostitution (Albini et al., 1995; Shelley, 1995) and instead turned to legitimise their activities by manipulating the political environment (Galeotti, 2004) in which they are operating, and once again building upon the political-criminal nexus established in the decades previously.

The fall of the Soviet Union and the push to privatise public assets provided Russian organised crime groups with the opportunity to capitalise on these rapid changes and influence their way to economic legitimacy (Dean et al., 2010; Galeotti, 2004; Marine, 2006); a concept coined by Vadim Volkov as “violent entrepreneurship” (Galeotti, 2004: pp. 57). Galeotti (2004) reaffirms the continuing trend amongst Russian organised crime groups, emphasising their ability to adapt to changes within their landscape, providing the groups with new opportunities for illicit activities while still maintaining their power. Notably, despite the adaptable nature of Russian organised crime groups, not all crime groups have successfully emulated their flexible characteristics, as seen during Cosa Nostra’s eventual demise in the United States following changes in the markets they once exploited (Jacobs, 2020).

The collapse of the USSR additionally opened the country to the global criminal marketplace, providing Russian organised crime groups with the opportunity to expand their operations. Long gone were the days of small-time cons and protection rackets; Russian organised crime was now able to dominate transnational crime (Shinar, 2016). Transnationality and the introduction of the internet provided Russian crime groups with the ability to seize new opportunities on a global scale; an example of these new opportunities includes the partnership between the Russian *mafiya* and Japanese Yakuza to supply prostitutes within Japan, which would eventually lead to the Russian *mafiya* running their own prostitution ring in Japan (Galeotti, 2004). Additionally, Russian organised crime groups took to the internet to expand their operations globally with organised crime through using online marketplaces to participate in international prostitute trades (Millar, 2000). Arguably, strategic alliances between organised crime groups are not uniquely Russian; transnational drug trafficking partnerships have existed between Mexican and Chinese organised crime groups (Bright and Leiva, 2021) and the Italian Mafia and Colombia drug cartels (Bargent, 2013). However, Russian organised crime differed from other organised crime groups when the features and motivations for transnationality were examined.

Russian organised crime groups were focused on being a vital feature of the global underworld (Galeotti, 2018b). While Russian organised crime would play key roles in the drug and weapon trade, similar to other criminal syndicates; organised crime

groups were also heavily involved in money laundering, the production of forged goods (Galeotti, 1998) and the seizure of profitable economic spheres (Cheloukhine et al., 2021). Notably, a key influence in the appeal of transnational crime to Russian organised crimes lies political and economic instability that existed following the collapse of the USSR. Cheloukhine et al. (2021) suggest that the transnationality of Russian organised crime was uniquely influenced by the rapid privatisation and close interconnection between illegal structures and transnational corporations, such as banks, public foundations, and private enterprises. This interconnection allowed organised crime groups to launder money and allowed for the criminalisation of the Russian economy.

Furthermore, transnational crime caused a shift in the recruiting practices of Russian organised crime groups. As global prospects arose, Russian organised crime groups shifted from recruiting “bulls (fighters, low-rank members of organised crime)” (Cheloukhine, 2008: pp 371) to instead hiring lawyers and other high-value and skilled professionals (Cheloukhine, 2008). This shift in recruitment aimed to legitimise the operations of these crime groups within Russian society (Siegel, 2012) and further improve their connections with the political elite. Using the professional knowledge of their new skilled members and the benefits provided by transnationality, Russian crime groups could intertwine themselves with foreign companies to conceal their operations and the origin of their capital (Cheloukhine, 2008, 2012) and influence foreign politics. However, Russian organised crime groups utilised these skilled professionals not just for legitimising their business but also in a variety of crimes, including the creation of slush funds (Gottschalk, 2010), financial manipulations, exploiting financial systems (Wheatley, 2021) and the corruption of state officials through lobbies (Varese, 2001).

The evolution of traditional Russian organised crime groups is highly unique and heavily influenced by politics, culture, and socioeconomics. While the aspect of the evolution of traditional organised crime groups would play a role in the later adoption of RaaS by Russian organised crime, the key influences would occur in the evolution of modern Russian crime groups.

3.3 Contemporary Russian Organised Crime

Following the fall of the Soviet Union, there was a notable transition for Russian organised crime from the traditional to the modern. This section will examine the key factors that discern the modern Russian criminal syndicates from traditional organised crime groups of the USSR and the path taken by Russian organised crime groups towards RaaS. Particularly, this section will examine further the underlying factors that heavily influenced contemporary Russian organised crime; the political-criminal nexus and socio-technological impacts.

3.3.1 Modern Criminal Recruitment

The shift in recruitment practices established by Cheloukhine (2008) is argued to be the catalyst in the transformation of 'traditional' Russian organised crime groups into their 'contemporary' counterpart. Through the change in the dynamics and personnel, the new generation of Russian crime groups moved away from the traditions and brotherhoods established during the time of *vory v zakone* and have shifted to a more corporate approach to crime (Lavorgna, 2019) with the desire for more significant profits, efficiency, and ultimate power the driving force behind this change. Siegel (2012) expands on the idea of the modern criminal business and highlights that since 2010, Russian organised crime groups have moved away from recruiting solely in prisons and aimed to fill their sophisticated criminal enterprises with educated professionals, including computer specialists, chemists, and intelligence experts.

The cause for the changes in recruiting practices is likely a result of a combination of factors. However, the two leading influences of the shift were an increase in the number of skilled professionals lacking employment following the fall of the USSR and the formalisation of organised crime toward a business model (Dremliuga et al., 2020). While the practice of recruiting skilled professionals was not a new concept; Cosa Nostra had recruited lawyers within their ranks in the past (Pace and Styles, 1975), and medical personnel have played a role in organised organ trafficking operations (Boll-Stiftung and Schonenberg, 2013); Russian organised crime groups

put a new spin on the recruitment practice as a result of their push towards formalisations.

Semyon Mogilevich is a clear example of Russian organised crime's recruitment of skilled professionals. Semyon Mogilevich, an early adopter of the new recruitment strategy, is a major Russian crime boss with close ties to the organised crime group *Solntsevskaya Bratva* (Siegel, 2012). Through recruiting specialists, Mogilevich's crime groups could conduct a range of sophisticated crimes, including several cybercrimes, activities that crime groups had not widely utilised prior to these changes in recruitment (Siegel 2012). Unlike previous instances where organised crime involved skilled professionals, these professionals were often a means to an end; Russian organised crime groups like Mogilevich's would bring these professionals to the forefront of their enterprises to conduct specialised crimes. Notably, while Russian organised crime groups like Mogilevich's pivoted to recruiting individuals that specialised in cybercrime in the early to mid-2000s, other traditional organised crime groups did not, with Cosa Nostra not become actively involved in cybercrime at a similar scale as Russian organised crime until over a decade later (Vavra, 2021).

The profits made from just one of these specialised illicit activities are significant due to the "high reward" (Siegal, 2012: pp 41, Tropina, 2013: pp 48) nature of the crimes, with some cybercrimes resulting in multimillion-dollar profits (Lavorgna, 2019; Siegal, 2012). Due to the nature of these specialised illicit crimes, particularly cybercrime, apprehending individuals within these organised crime groups is more challenging, a prospect that is undeniably appealing to Russian organised crime syndicates (Choo and Grabosky, 2013; Broadhurst et al., 2014; Ortner, 2015). Distinctively, the shift in the recruiting practices of modern Russian organised crime groups provided criminal syndicates further opportunities to legitimise themselves in the eyes of the Russian state and would contribute to their heightened influence in the years to come. While organised crime groups would utilise the recruitment of skilled professionals to commit various crimes, the adoption of cybercrime would significantly increase the shift in recruiting practices.

3.3.2 Russian Organised Cybercrime

The notable shift in recruitment combined with the draw of 'high reward' crimes would contribute to Russian organised crime groups' noteworthy adoption of cybercrime activities. However, additional factors contributed to the shift by Russian organised crime groups to cybercrime, including cultural changes within Russia, the growth of new technology and socioeconomic influences. Just as the *vory* shifted to extortion and fraudulent schemes during the Brezhnev era (Albini et al., 1995), the shift by Russian organised crime was just an extension of the *vory v zakone's* fundamental crime pillar of gaining a profit in the most effective way possible. The adoption of new technology and cybercrime provided organised crime groups with a plethora of new profit avenues, with Russian cybercrime syndicates accumulating over 1.9 billion dollars in 2013 alone (Leukfeldt et al., 2017; Ortner, 2015).

Arguably, the adoption of new technology such as computers and the dark web were not new concepts for Russian organised crime groups, with new technology being embraced following the fall of the Soviet Union. However, Russian organised crime groups' adoption of new technology caused a notable cultural shift; while monetary motivations still existed, the groups were also powered by broader external factors, including intellectual challenges and rebellion against Western adversaries (Grabosky, 2015). Beyond the cultural shift caused by new technology, the rapid growth of technology within Russia created a gap in the policing of cybercrime, an appealing prospect to Russian organised crime groups. While further analysis of legislative gaps' impact on the growth of cybercrime will occur in a later chapter, notably, Russia's lack of effective cybercrime policing caused the dramatic increase in its adoption by organised crime.

Russian cybercrime legislation focused solely on protecting Russian-based victims, leading organised crime groups to attack Western-based targets instead (Uchill, 2022). The prominent gap within the legislation resulted in the growth of Russian cybercrime, with Russian becoming the home of the most advanced organised cybercrime groups that have stolen billions of dollars from Western victims (Lewis, 2022). Furthermore, Russian organised crime groups have exploited the Russian government and the FSB's refusal to arrest cybercrime groups (Grabosky, 2016; Ortner, 2015), utilising the impunity provided to cybercrimes to conduct highly profitable organised cybercrime businesses. Evidence of the impunity provided to

Russian cybercriminals is profound, with arrests rarely occurring and the Kremlin preventing the extradition of Russian cyber criminals to the United States (Stone, 2020).

In addition to the appeal of ‘high reward’ and impunity, Russian organised crime groups turned towards cybercrime due to the creation of a generation of information technology specialists resulting from Russia’s advanced technology capabilities (Ortner, 2015, Maurer, 2017). Socio-technological influences would play a vital role in the adoption of cybercrime by Russian organised crime groups. Russia developed a generation of highly skilled information technology professionals from the 1980s to the early 2000s; however, due to high competition and low wages within the I.T. sector, many of these skilled individuals could not find stable employment (Maurer, 2017). Russian organised crime groups would utilise this opportunity and competitively recruit high-quality technology specialists to conduct cybercrime activities.

The Russian Business Network (RBN) was a significant player in Russian organised crimes adoption of cybercrime. Purportedly conducting sixty per cent of internet crime in 2007 (Warren, 2007), the Russian Business Network highlights how Russian organised crime had been perfectly situated to conduct cybercrime due to the competitive unemployment landscape in post-Soviet Russia and the potential influence of the Russian government (Warren, 2007). Further analysis into the impact of the socio-technological and political influences on Russian organised crimes adoption of RaaS will occur in a later chapter; however, the effects of socioeconomics and technological advances on organised crime are significant and have played a role in Russian organised crime adoption of cybercrime and eventually RaaS.

3.3.3 Organised Crime and the State

Vaksberg (1991) argued that the title of Russia’s titular organised crime syndicate is not held by criminals that hide in the underbelly but by the politicians pulling the strings in plain view. They argue that in Russia, politicians use criminal methods to preserve power and maintain their stronghold over the state. While this argument

was developed long before the establishment of modern Russian organised crime syndicates, it continues to ring true more now than ever.

While later chapters will further analyse the relationship between the political elite and Russian organised crime, it is worth calling out the nexus between the two groups. Russian organised crime groups and the state have developed a strong relationship following the fall of the USSR, with the two working together through a continual exchange of power (Galeotti, 2018a). Contemporary Russian organised crime groups would infiltrate all areas of government (Cheloukhine and Haberfeld, 2011), from local government to the Kremlin, in a bid to maintain power and control. Through this infiltration, the symbiosis between the Russian state and organised crime was complete, and the criminal world could influence the Kremlin.

The rise of Vladimir Putin has seen the growth of a corrupt environment conducive to building the relationship between organised crime and the state. The rise of Vladimir Putin would cause a substantial shift in the socio-political landscape of Russia due to the expansion of strategic corruption, the adoption of kleptocratic tactics, the restoration of aspects of the Soviet power model (Lanskoy and Myles-Primakof, 2018), and military aggression. The shift in the socio-political landscape would aid in strengthening the government's relationship with organised crime as the political-criminal nexus benefited their socio-political thievery. Russian organised crime groups conduct illicit activities on behalf of the Kremlin (Galeotti, 2018b) and state agents utilise the political-criminal nexus for their own political and monetary gain. The strength of the nexus was evident in the arrest of high-ranking police colonel Dmitry Zakharchenko in 2016 on corruption charges due to his relationship with organised crime syndicates (Saric, 2019). Overall, the connection between organised crime and the political elite in Russia is a relationship that revolves around mutual profits and the maintaining of control. Chapter three will analyse the significance of Putin to the evolution of Russian organised crime toward RaaS in further detail. However, the relationship between Russian organised crime and the state would play a significant role in the later evolution of Russian organised crime as it would establish the precedent of organised cybercrime groups acting on behalf of the state, including RaaS.

3.3.4 State Sponsored Russian Cybercrime

While socio-technical influences in the form of new technology had a significant impact on the development of Russian organised crime, the most considerable influence on organised crime would be the political-criminal nexus. As the state and organised crime groups became more intertwined over time, the most significant evolution of organised crime appeared with the introduction of state-sponsored organised cybercrime. Arguably, state-sponsored cybercrime was a continuation of the state's involvement within criminal activity that existed since Brezhnev; however, the tactics used by the Russian state are new. Cyberwarfare and the utilisation of organised crime groups to conduct cyberattacks has been a tool increasingly exploited by the Russian government to maintain control within the country and to threaten Russian adversaries. While organised crime groups have utilised cybercrime as a profit stream, the growth of state-sponsored organised cybercrime has had a lasting impact on Russian organised crime and has contributed to the growth of RaaS in Russia.

Grabosky (2015) highlights that state-sponsored organised crime can incorporate different levels of cooperation between crime groups and governments. The state's involvement in organised crime ranges from the government turning a blind eye to criminal activity to the government's significant involvement in criminal activity through either active sponsorship or formal cooperation (Grabosky, 2015; Karstedt, 2014). In the case of Russian state-sponsored organised cybercrime, the Russian government has collaborated with "patriotic hackers" to support each other's interests (Grabosky, 2015). Evidence of active Russian sponsorship of "patriotic hackers" includes the establishment of the espionage group Fancy Bear. Linked to the Russian government, Fancy Bear has carried out several politically motivated cyber-attacks, including an attack on the Democratic National Committee in 2016 and a United States nuclear facility in 2017 (Galeotti, 2017; Greenberg, 2019; MITRE ATT&CK, 2021; TeamPassword, 2021).

Additionally, the Russian state has turned a blind eye or encouraged several "patriotic hacker" groups that have conducted activities in support of the state. These groups include the cybercrime group *Wizard Spider* (also known as *Trickbot*), which conducts ransomware activities against non-Russian targets and is not discouraged

by the Russian government (Lally, 2021) and *Conti*, the RaaS group conducting ransomware activities in support of the Russian government following the invasion of Ukraine in early 2022 (Burgess, 2022). Arguably, the Russian state's heavy investment in cybercrime and the recruitment of "patriotic hackers" is merely a continuation of the fears that existed following Gorbachev's reforms; that they would lose control within Russia and there must cling to whatever power, they can.

This rise of Russian state-sponsored organised cybercrime can be linked to Vaksberg's (1991) argument regarding the political elite's desire to maintain power at any cost. As the political elite, including Vladimir Putin, fought to preserve their stronghold, widespread corruption within Russian increased (Transparency International, 2021), and the collusion with organised cybercrime was conceptualised and gained a foothold (Karstedt, 2014). While Vaksberg's argument referred to the political landscape at the fall of the USSR, their argument highlights the persistence of the relationship between organised crime and politics within Russia. While state-sponsored organised crime is nothing new, previous research has examined the political-criminal nexus (McCarthy-Jones and Turner, 2021; Paoli, 2015); the Russian government's involvement and wilful ignorance of Russian organised cybercrime groups have brought new insight into the concept. While arguably other nations are involved in state-sponsored cybercrime, most notably North Korea's Lazarus Group (Park, 2021), Russia's state involvement in cybercrime spans longer than other states and has motivations that are more complex than North Korea's simple desire for financing (Park, 2021) with the desire for total control a leading influence.

From the days of the *vory v zakone* to the modern state-sponsored organised crime groups, Russian organised crime groups have been heavily influenced by the political-criminal nexus and socio-technological impacts. This chapter examined Russian organised crimes' unique history and the notable shifts in their evolution that led them towards RaaS. While this chapter explored the role of politics, culture, technology, and socioeconomics in contributing to the evolution of organised crime towards RaaS, the following chapters consider in further depth the political and socio-technological influences that have supported the growth of RaaS in Russia.

As can be see, the landscape within Russia has been uniquely suitable for the growth of RaaS due to the connection between organised crime and the Russian state. This chapter has explored Russian organised crime's history and the shift towards RaaS by examining the political-criminal nexus and socio-technological influences. It examined the role of the Russian state in the evolution of organised crime and analysed how the developing relationship between organised crime and the state created an environment permissive to RaaS. The next chapter further analyses the scale on which the state has contributed to the growth of RaaS within Russia.

The Russian Political Landscape and the Cultivation of RaaS

Russia has long been the nexus of cybercrime, with experts arguing that Russian hackers are the best in the world (Segal, 2016; Frye, 2021) due to their significant footprint within the cybercrime space, with almost sixty per cent of hacking attempts

linked to Russian hackers (Lyngaas, 2021). While Russia has been the leading source of cybercrime well before the rise of RaaS (Lewis, 2022), with Russian hackers using their tools to sway public opinion during elections and infiltrating private organisations and governments (Fyre, 2021), there is a notable gap within the literature's understanding of why Russia has become a haven for RaaS and ransomware groups. Russia's political landscape, beginning from the Cold War, has shaped how Russia not only addresses ransomware groups but also contributed to the growth of RaaS within the nation.

This chapter goes beyond and current literature and explores the key areas within Russia's political ecosystem that have made Russia an environment permissive to RaaS. Specifically, this chapter posits that the growth of RaaS in Russia is a direct result of the Russian government through deliberate involvement and purposeful non-intervention. Furthermore, this chapter argues that the Russian political elites created an environment permissive to RaaS through a legacy of a corrupt political landscape, ineffective cyber legislation and policing, and their active and aggressive commitment to state-sponsored cyberwarfare. While previous knowledge has examined Russian role within the cyber landscape, it is through an examination of the impact that corruption, Vladimir Putin, the political-criminal nexus, cybercrime policy, and state-sponsored cyber warfare have played in cultivating RaaS, that the scale at which the state is involved within RaaS is evident. As the growth and capabilities of RaaS groups continue to grow, those with the cyber security landscape must understand the factors beyond the technical influences that have contributed to the growth.

4.1 Corruption in Russia

As proposed by Holmes (2008), corruption, organised crime, and the Russian government are and have always been interconnected. Ranking 136 out of 180 countries on the Corruption Perceptions Index (Transparency International, 2022), which places Russian next to Libera and Pakistan, and 118 positions below Australia, evidence is clear that compared to many other nations, the Russian state is highly corrupt as a result of political elite shifting the balance of power. A key point to consider is that this level of corruption within Russia is not new, with political

corruption in the form of bribes, report padding, embezzlement and the abuse of authority all common occurrence in the USSR amongst Communist Party bosses and law enforcement (Galeotti, 2018; Schwartz, 1979).

The level of corruption within Russia is large in scale and influences society on a multitude of levels. Corrupt billionaire oligarchs have appropriated resources including seizing smaller businesses to keep Russia's economic power in a limited number of hands (Lanskoy and Myles-Primakoff, 2018) to a detriment to the wider Russian population. Furthermore, the Russian government have used ruthless violence to protect and bolster their interests (Galeotti, 2018b), including the assassination of political enemies that pose a threat to the dysfunctional elites (Harding, 2020) and the invasion of Ukraine to further their control within the state (Idris, 2022). While these corrupt activities are significant, arguably the most substantial impact of this corrupt landscape lies in how entwined it has become within Russia and how it has become the norm in Russian society.

According to a survey of public opinion in Russia in 2012, the Russian public deemed the level of corruption within the state as high or very high (Cheloukhine et al., 2021), highlighting the scale in which corruption is occurring within the state. These opinions are substantiated by the corrupt activities seen often within Russia, including the exchange of information between government officials and organised crime groups (Cheloukhine et al., 2021), the raiding of social budgets for personal gain (Dawisha, 2014) and the acceptance of bribes by the political elite for favours (Schulze et al., 2016). The corrupt environment in Russia has not only become the norm of daily life for those within all spheres of society for the last century (Cheloukhine et al., 2021) but has provided organised cybercrime groups with the ability to manipulate the environment to their advantage.

Corruption within Russia has contributed dramatically to the state becoming the breeding ground for RaaS, notably due to the neo-feudal capitalist dogma that has become prominent within Russian politics. Russian neo-feudal capitalism is a system where the elite have seized power and law (Kuttner and Stone, 2020), resulting in extreme inequality and "unassailable barriers" to class mobility (Dean, 2020). A system that embraces corruption within its government (Gragido et al., 2013) and

emphasises the feudal inequality model (Åslund, 2017). While the political elite have created a system that uplifted their own power, so too had they created a system that RaaS groups could manipulate.

Organised cybercrime's manipulation of the corruption within the Kremlin is evident when examining the RaaS group Evil Corp. Evidence had shown that Evil Corp's connection to the Russian government, with one member, reportedly working for the FSB while also preserving connections to high-ranking FSB members (United States Department of the Treasury, 2019; DiMaggio, 2021), all while they participate in ransomware activities. When combined with the evidence of the Kremlin purposely building relationships with ransomware group members (Burgess, 2022), it is apparent that the Kremlin and ransomware groups are manipulating the corrupt political system constructed by the corrupt Russian government for their personal enrichment, which has allowed RaaS to thrive in Russia (Tucker, 2021).

Remarkably, the Russian people have viewed corruption as a somewhat acceptable societal norm, which has contributed to a lack of meaningful laws targeting corruption (Beck and Lee, 2002; Holmes, 2008). The Kremlin and RaaS groups have abused this acceptance within society to continue their corrupt political-criminal relationship. While bribes and favours have benefitted both the political elite and organised crime groups, the corruption that has benefitted RaaS groups runs deeper. Specifically, the Russian political elite created inconsistencies within legislation to deteriorate the socioeconomic and political landscape for their personal gain, inconsistencies which RaaS groups have exploited to ensure their survival.

Few corruption-related arrests have occurred under Putin's leadership, with the most notable arrests including that of the oligarch Vladimir Yevtushenkov (Rankin, 2014) and politicians Alexei Ulyukayev (Nikolskaya and Korsunskaya, 2017) and Aleksandr Khoroshavin (Radio Free Europe, 2022). Arguably these arrests occurred at the behest of the Kremlin to bolster the economic and political power of Putin as the oligarchical powers of these dysfunctional elites grew (The Economist, 2017). The few arrests that have occurred are merely an example of the scale in which corruption exists within Russia.

Notably, Russia has not conducted any large-scale arrests relating to corruption between the political elite and organised cybercrime groups. In contrast, organisations, including INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC), have arrested thousands of individuals connected to cybercrime and corruption activities, including three thousand during a 2022 operation (INTERPOL, 2022). The arrests efforts in Russia instead have focused on Putin's political opponents, underscoring the Kremlin's rampant corruption (Dawisha, 2014; Bennetts, 2018) and highlighting to ninety-five per cent of the Russian population that the Kremlin’s anticorruption efforts are not serious (Dawisha, 2014). The Russian government has created a system where corruption is supported so long as it continues to meet the needs of the elite. RaaS groups have grown within Russia by simply manipulating the corrupt system established by the elite by ensuring they are dismissed so that their activities support the needs of the elite.

4.2 The Reign of Vladimir Putin

Within the last issue of Kommunist (the mouthpiece of the USSR's Central Committee) was the clear message that although the USSR was collapsing, as far as the KGB was concerned, their conservative agenda would remain unchanged (Shlapentokh, 1993). While it would be nine years between this statement and Vladimir Putin coming to power, it is a sentiment that provides insight into Putin's reign and his political agenda. Working within the KGB as an intelligence officer (Hoffman, 2000), Putin's time within the KGB would inadvertently contribute to creating an environment where RaaS has flourished in Russia. During his time in the KGB, Putin would utilise 'active measures' to disrupt or disable Soviet adversaries (Belton, 2020). These measures would evolve from misinformation and assassinations to the use of cyber warfare and ransomware.

Putin and the Kremlin have supported RaaS groups as these groups have enabled Russia to utilise further 'active measures' to disrupt adversary nations' systems while adding a layer of removed accountability for the Russian government (Horsley, 2019). These disruptive activities include the outage of a Ukrainian power grid (Zetter, 2015) and the Italian energy sector (Lepido, Gallagher and Brambilla, 2022). Evidence of Putin's support of RaaS groups is made clear by the Australian Cyber

Security Centre (2022c), which contends that the KGB's successor and organisation that Putin has direct control over (Schneider, 2008), the FSB, have tasked ransomware groups to carry out disruptive ransomware attacks on Russian adversaries. Without Putin and the FSB's support, RaaS groups would not have likely grown to the scale they have; it is organised cybercrimes' partnership with Putin has allowed RaaS to flourish in Russia.

Furthermore, Putin's time within the KGB and the FSB has contributed to the growth of RaaS in Russia due to the strict nationalist practices built into the agencies coupled with the massive network of former FSB and KGB officers influencing his leadership. An estimated seventy-six per cent of politicians surrounding Putin held positions within the KGB and FSB (Global Security, 2022), emphasising the scale on which they have entwined themselves with Putin. With this large-scale influence, the FSB ideals have dominated Putin's agenda, with their focus on provoking and escalating tensions with adversaries (Roth, 2022) to increase the power and control of the political elite.

Throughout Putin's time in power, there has been a continual progression toward stronger conservative and authoritarian ideologies (March, 2012; Fenghi, 2020), including blaming the West for troubles within Russia, the introduction of wedge issues within politics and the push for a united Russia (Hale, 2016). Arguably this progression has become even more apparent since Putin's return to the Presidency in 2012 (Suslov and Uzlaner, 2020) and Russia's annexation of Crimea in 2014 (Kaylan, 2014), with Putin implementing full-fledged conservative policies. With the implementation of staunch isolationist and authoritarian policies (Belton, 2020; Suslov, 2020), including harbouring the leaders of criminal organisations (Belton, 2020) and the militarisation of Russia, Putin created an environment where information confrontation against adversaries has become the norm (Fenghi, 2020; Hakala and Melnychuk, 2021). Furthermore, the emphasis on ideologies that placed Russian interests above all else contributed to an environment permissive to RaaS as it demonstrated to RaaS groups that so long as Russia profited and the West suffered, their destructive activities would be tolerated.

The implementation of consistent conservative policies has created an environment within Russia where RaaS has been able to take a foothold as it has created a landscape in which cybercrime activities are viewed as information confrontations that benefit Putin and Russia while undermining adversary nations. Through Putin's conservative and nationalist rhetoric, which underscores that Russia must be united against the West, Putin has created a landscape that promotes actions that are a detriment to their adversaries. Just as the invasion of Ukraine is a display of Russia and Putin's nationalist ideals, so is Russia's permissiveness to RaaS as it is a tool for Russians to unite against their perceived enemy. Putin and his authoritarian regime have allowed RaaS to grow as it directly coincides with the conservative dogma regarding Russia gaining tactical, economic and intelligence advantage over adversaries by utilising irregular warfare approaches such as cyber warfare (Potter, 2016; Svendsen, 2018).

Like the corruption that arose in the USSR and the years following its collapse, Putin's reign of crime and corruption has contributed to the growth of RaaS within the nation as it has permitted criminal activity and organised crime groups to be at a minimum swept under the rug as long as the bribe is well placed; and at best, created an environment where ransomware has been entrenched within the Kremlin (National Cyber Security Centre, 2018; The Associated Press, 2021; Australian Cyber Security Centre, 2022). By cultivating a corrupt environment where criminal activity is acceptable, Putin has, in turn, created an environment where RaaS is also acceptable.

4.3 The Russian Political-Criminal Nexus

While there are specific aspects of Russian organised crime's evolution that have contributed to the growth of RaaS within Russia, one aspect of Russian organised crime that has stayed consistent throughout its evolution and has contributed to the rise of RaaS is the relationship between organised crime groups and the political elite. Since the days of the *vory v zakone*, there have been corrupt relationships between organised crime groups, politicians, and law enforcement. This section will examine how the political-criminal nexus has contributed to the growth of RaaS.

As outlined previously, Russian organised crime groups would employ a variety of efforts to develop relationships with prominent members of the Russian political elite to ensure their activities could continue with little interference; these efforts, including bribes, intimidation, and favours, would be utilised to influence those in power, including those within law enforcement. Due to limited resources, poor training, and meagre salaries (Galeotti, 2018b), law enforcement within Russia became an easily corrupted institute for organised crime to manipulate. Traditional organised crime groups would form relationships with law enforcement members, including key KGB members, to ensure their activities remain unimpeached. Rampant corruption as a result of non-existent checks and balances and a corrupt culture provided organised crime groups with the ability to develop close relationships with key members of law enforcement, as evidenced by the mutually beneficial relationship established between organised crime groups and the KGB during the 1980s and 1990s (Galeotti, 2018b).

Furthermore, organised crime groups, including the *vory v zakone,* would accept members of the KGB within their ranks, a way for organised crime groups to influence those in power while providing the KGB with the ability to monitor the criminal underworld (Glenny, 2008). While intelligence organisations and organised crime groups have worked in tandem in the past, most notably the American Mafia and the CIA in the early 1960s (Wolske, 2000), the deep-rooted connection between the Russian intelligence agencies and organised crime groups is unique. The engrained relationship between law enforcement and organised crime groups continues today, with Russian organised crime groups, including RaaS groups working together with the FSB (Zabrisky, 2020). By creating a unique environment where relationships between organised crime and law enforcement existed and were supported, RaaS groups could grow without obstruction from those tasked with preventing their criminal activities.

Russian organised crime and the Russian government partnership have been long-standing, with the *mafiya's* influence reaching the highest level of the Kremlin (Boylan, 1995; Chêne, 2008). Reports of Russian organised crime's connection to high-level members of the Kremlin are extensive, with some arguing that even Vladimir Putin worked with the organised crime group Tambov-Malyshev during the

1990s (Zabrisky, 2020). Russian organised crime groups distinctively maintained relationships with the elite within the Russian government to expand the reach of their power and ensure their criminal activity continued uninterrupted. As highlighted by Galeotti (2017; 2018a; 2018b) and Naím (2012), organised crime groups and the Kremlin's relationship was often an exchange of power, with organised crime groups conducting activities on behalf of the Kremlin, including assassinating political targets and conducting intelligence activities (Galeotti, 2017). Through these exchanges, organised crime groups and the Kremlin ensured their overall power within Russia remained unencumbered.

RaaS groups have utilised the same techniques as traditional organised crime groups in forming a nexus with the Russian government, as evidenced in the 60,000 leaked messages from the RaaS group *Conti* in early 2022, which emphasises not only the relationship between RaaS groups and the Kremlin but also the exchange of power that once again exists between the two (Burgess, 2022; Faife, 2022). Without the precedent created by organised crime groups, it can be argued that ransomware groups would not have formed the power exchange relationships with the political elite within the Kremlin, and RaaS would not have flourished within Russia.

4.4 Russian Cyber Legislation

While political agendas and corruption have significantly contributed to the growth of RaaS in Russia, specific aspects of Russia's cyber-related policies have supported organised crime groups in creating an environment where RaaS has flourished. This section will analyse how loopholes within cyber legislation have made RaaS appealing within Russia. Russia's 1996 Criminal Code, the primary source of criminal law within Russia, covered several areas relating to cybercrime, including articles pertaining to illegal access to computer information and the violation of rules regarding computers and networks (Dremliuga et al., 2020). However, while legislation exists around cybercrimes, there was a lack of law enforcement involvement regarding cybercrime in the late 90s to early 2000s, a stark contrast to the United States' Computer Fraud and Abuse Act which was enacted in 1984 (Eichten, 2010). Instead, the Russian government largely ignored cybercrime compared to other crimes such as financial or organised crime (Dremliuga et al.,

2020). This original law and the resulting inaction from the government would lay the foundation for RaaS growth within Russia.

While revisions to provisions within the Criminal Code occurred following the rise of cybercrime and the increased financial damage it caused, inaction would continue, with the number of arrests relating to cybercrimes decreasing from nearly 10,000 in the mid-2000s to less than 2,000 in 2016. (Latypova et al., 2019). While some within Russia may argue that this decrease in arrests proves that law enforcement has prevailed over cybercrime, it merely highlights that Russia has created an environment where cybercrime can be conducted without the fear of arrests and would reinforce the argument that Russia created an environment where cybercrimes like RaaS are perpetrated without constraint.

Within Russia's cybercrime policy, there are legal loopholes that, due to a fundamental disinterest in rectifying the gaps (Gragido et al., 2013), have continued to be abused by RaaS groups. These loopholes, including the creation of a law enforcement system that was unable to prosecute cybercriminals (Gragido et al., 2013), provided a rich environment where RaaS could develop, allowing organised crime groups to work around the edge of the law to avoid arrest. A notable example of a legal loophole exploited by RaaS groups lies within Russia's Sovereign Internet Law, which on the surface, aimed to force internet traffic through monitored internet exchanges (Chislova and Sokolova, 2021); however, the law was built with flaws. To prosecute a cybercriminal under the Sovereign Internet Law, the attack must be against a Russian target. RaaS groups have learnt that by attacking Western targets and avoiding all Russian-based ones, they can avoid arrest under the law and can conduct their activities freely (Kundaliya, 2019). By creating laws that have these gaps, the Russian government have made RaaS permissible in Russia as there are no consequences to their illegal activities.

Ransomware groups and the FSB have abused the loopholes within Russia's cybercrime laws. A clear example of this exploitation by the FSB is apparent in the recent arrest of members of the RaaS group REvil. The FSB arrested several members of the ransomware group REvil in January 2022 after mounting pressure from the international community (Saarinen, 2022). However, following the arrest, no

further action against the members has occurred, with the Russian media outlet Kommersant reporting in June 2022 that due to a lack of further cooperation from the United States intelligence community, the members of REvil are unlikely to be charged (Marks, 2022).

Furthermore, the FSB has abused these loopholes by providing safe houses for hackers being perused by Western nations, as the Russian government views the hackers as valuable assets (Meduza, 2018). The legal inaction and exploitation further reinforce that the Russian government has created an environment where legal loopholes exist to ensure that no substantial penalty occurs for those conducting RaaS, making Russia a highly appealing environment for organised crime groups conducting RaaS.

4.5 State Sponsored Cyber-attacks

The Russian military and intelligence community have a long-running career of utilising cyber warfare as part of their military policy. While cyber warfare includes acts of cyber espionage and surveillance (Grabosky, 2016), the leading form that has contributed to the growth of RaaS in Russia is offensive cyber-attacks. The earliest records of the Russian government's use of cyber warfare occurred in 2007, with Russia conducting distributed denial of service attacks (DDoS) against the Estonian government (Grabosky, 2016; Frye, 2021). This attack was the first display of Russia's willingness to misbehave in cyberspace (Tamkin, 2017) and set the stage for acceptable cyber activities within Russia. The next notable event was the aforementioned 2017 NotPetya ransomware attack created by the cybercrime group Sandworm (Greenberg, 2019). NotPetya marks the first instance of a Russian military cyber-attack reaching far beyond its original target (Greenberg, 2019) but would be the first large-scale use of ransomware by Russia.

By examining the growth of RaaS groups in Russia since their adoption of state-sponsored cyber-attacks and, in particular, the NotPetya attack, evidence shows that many of these groups formed following the NotPetya, including the first iterations of *RansomExx*, *Conti* and *Grief* (Feeley and Hartley, 2019; Krebs, 2021c; Trend Micro Research, 2021a). Through their display of ransomware as a tool of cyberwarfare,

the Russian government indicated to organised cybercrime groups that RaaS was an acceptable cybercrime so long as the Russian enemy was the target.

While Russia's cyber warfare attacks were not conducted by RaaS groups, they did create a precedent where the use of cybercrime is an acceptable activity within Russia. As highlighted by Frye (2021), and Soldatov and Borogan (2015), the Russian government employs not only security and military to conduct its cyber warfare but also recruits freelance hackers and hackers that specialise in financial cybercrime, as these hackers would provide the Kremlin with a level of deniability as well as provide a wealth of knowledge. This deniability provides the Russian state with a layer of protection from geopolitical repercussions and accountability while ensure their political objectives are met. Through the utilisation of freelancer specialised hackers, the Russian government created a direct connection to hackers within their political environment (Soldatov and Borogan, 2015). The relationship between cyber criminals and the Kremlin has played a key part in Russia's cultivation of RaaS groups. The relationship has guaranteed that organised cybercrime activity is ignored or even promoted by the Kremlin so long as the Kremlin's interests are maintained. Furthermore, through the Kremlin's historical propensities of supporting "pro-Kremlin cyberwarriors" (Frye, 2021, pp: 188), it is apparent that the Russian government, through their manipulations within the political ecosystem, have created an environment where becoming a cybercriminal that utilises RaaS is appealing and safe undertaking.

This chapter posited that the growth of RaaS in Russia is a direct result of the Russian government through deliberation involvement and purposeful non-intervention. It examined the role of the Russian political elites in creating an environment permissive to RaaS through a legacy of a corrupt political landscape, ineffective cyber legislation and policing, and their active and aggressive commitment to state-sponsored cyberwarfare. The next chapter considers the socio-technological influences that have contributed to the growth of Russian RaaS groups and seeks to understand the impact that the environment created by the Russian state has had on the cultivation of ransomware in Russia.

Socio-technological Factors Influencing the Growth of Russian RaaS

Current research has attempted to unravel the determining factors of cybercrime; however, the existing literature around the factors contributing to cybercrimes, particularly RaaS, is limited and primarily focuses on technical perspectives (Park et al., 2019). Whilst the previous chapter argued that the growth of RaaS in Russia is a direct result of the Russian government, this chapter posits that there are socioeconomic and technical influences created by the Russian government that have contributed to the cultivation of RaaS within the state. This chapter argues that utilising the "socio-technological" lens (Yip et al., 2012; Broadhurst et al., 2013, pp. 16) is essential to understanding the true scope in which Russia has cultivated RaaS. Specifically, this chapter will argue that Russia's technological history and socioeconomics are significant components in forming an environment where RaaS has flourished within Russia. Through examining these influences, it becomes evident that Russia was destined to become the nexus of RaaS, just as it has for other forms of cybercrime. While previous literature has argued that the growth of cybercrimes, including ransomware, can be primarily attributed to the proliferation of botnets (Broadhurst et al., 2013); the influence of Russian technoculture, education and socioeconomics (Gragido et al., 2013) on organised cybercrime cannot be discounted.

5.1 The Socio-technological Lens

Yip et al. (2012) argue that cyber security and, in turn, cybercrime are often viewed as solely a technical problem, a problem that is the direct result of new technology emerging and providing cybercriminals new illicit opportunities. However, cybercrime should also be viewed as a socio-technological issue; that encompasses both

sociological and technological influences. An extension of affordance theory, which posits those conditions perceived within an environment offer the possibility for criminal actions (Hutchby, 2003), the socio-technological approach enables a balanced examination of the role of socioeconomic and technological determinism in contributing to harmful criminal behaviour Wood, 2021). While Wood (2021) contends that affordance theory and the use of the socio-technological lens can limit the analysis to just how technology is used to conduct crime, arguably, the approach provides a more holistic understanding of the conscious and unconscious impact that socioeconomics and technology have on cybercrime offending.

Explicitly, a socio-technological hybrid approach to understanding RaaS provides greater insight into how socioeconomics influences individuals and groups towards cybercrime but also how technology contributes to cybercrime offending as a result of shifts in acceptable social practices (Wood, 2021). By embracing a socio-technological lens when analysing the factors contributing to the growth of Russian RaaS, a deeper understanding of the role environment and behaviour play in cultivating cybercrimes is permitted. This deeper understanding is achieved by enabling the articulation of specific sociological and technological circumstances that have contributed to the growth of Russian RaaS.

Furthermore, the socio-technological lens provides a holistic understanding of the motivations behind the rapid adoption of RaaS in Russia beyond surface-level ideas, such as the availability of new technology. Additionally, through analysing the factors that have contributed to the cultivation of RaaS in Russia through a socio-technological lens rather than solely a technological lens, our understanding of the influences of cybercrime is not bound to the never-ending battle against technological advances (Yip et al., 2012). Previous research has demonstrated the merit of the socio-technological lens when examining cybercrime offending (Olayemi, 2014); therefore, this section aims to build upon previous research and utilise the approach to analyse the characteristics contributing to the cultivation of RaaS in Russia.

5.2 Russia's Technological History

The final years of the Soviet Union and the first years of the Russian Federation saw various technological transformations, with new skills, technology and underground societies forming during this period. The introduction of computer literacy (Kerr, 1991), the growth of computer ownership (Dremliuga et al., 2020) and the availability of foreign computer systems (Alexander, 1985) shifted how the Soviets interacted with technology. While the shifting interaction with technology has been mirrored by other countries, including China, in the 1980s and 1990s during their push towards scientific competitiveness (Zhang and Wang, 1995), the amalgamation of technological developments and societal relationships with technology within Russia are unique to the country. While seen as the tool to move the USSR and Russia in a new direction and towards the modern world (Kerr, 1991), growing technology and technology capabilities would eventually contribute to the growth of RaaS within Russia. This section will examine the influence of Russia's information technology history and the rise of the hacker subculture within Russia during the 1980s and 1990s in cultivating RaaS within the nation.

5.2.1 The Information Technology Cold War

In the mid-1980s, the USSR had between ten to eighty thousand computers, a fraction of the over a million computers in the United States (Bakarv, 2017; Williams, 2022). The Soviet government, painfully aware of their losing battle with information technology, shifted its priorities to developing its I.T. sector. The USSR, attempting to outpace the United States, invested heavily into STEM-based education fields, predominantly advanced mathematics and computer sciences (Gragido et al., 2013), eventually forming computer education programs that were amongst the best in the world (Dremliuga et al., 2020). While the push to improve the Soviet I.T. sector would provide Russia with a boost in education (Kerr, 1991), the attempt to beat the Americans would, however, eventually lead Russia toward the path of cybercrime and RaaS.

The emphasis on skilled I.T. professionals resulted in a pool of highly trained individuals competing to enter the workforce (Bakarv, 2017), with tens of thousands of computer sciences students graduating yearly (Bush, 2004). However, the

Soviet's I.T. sector did not have room for many of the skilled I.T. professionals (Dremliuga et al., 2020). Thus, individuals would either accept minimal paying positions, attempt to establish their own I.T. business under the radar (Dresen, 2022) or turn to cybercrime (Dremliuga et al., 2020). Unbeknownst to Russia, the push to expand STEM education in the 1980s to 1990s would have a flow-on effect on the number of unemployed computer literate individuals and would increase the number of individuals with the skills and knowledge to conduct cybercrimes, including RaaS.

While the increase in skilled professionals would contribute to the growth of RaaS in Russia, the increase in accessibility to new technologies would be a determining factor to the growth of RaaS within the country. As proposed by Park et al. (2019), internet connection speeds are positively related to the number of cybercrime perpetrators, highlighting the influence of technological determinism on cybercrime offending. In their attempt to catch up to the capabilities of the West, the Russian government aimed to increase the potential of the nation's internet (Baraniuk, 2016). Following the fall of the USSR, Russia experienced a dramatic growth of internet users, with the number of internet users, most notably adolescent users, quadrupling between 1996 and 2000; following this notable growth, there was a dramatic increase in cybercrime within Russia (Dremliuga et al., 2020).

Notably, China saw a similar consequence occur as access to new technology increased from the early 1990s to the late 2000s Wang and Li, 2012), which in turn has increased the scale of cybercrimes occurring within China, with the rates of cybercrime increasing thirty per cent a year (Bernard, 2020). While the impact of access to technology is not uniquely Russian, with the growth of the internet and the increased internet speeds in Russia, cybercrime has become significantly more accessible to skilled individuals. Furthermore, as Russia continued to build up its internet capabilities, so did the infrastructure required to conduct RaaS (Park et al., 2019). With the ability to easily access the internet and do so at faster speeds, Russia would become a haven for those desiring to conduct RaaS.

5.2.2 Soviet Hacker Subculture

Russia's technological history has contributed to the growth of RaaS due to the hacking subculture that has been prevalent in the country for over three decades.

Beginning in the 1980s, with the hacking of American software to run on Soviet machines (Delio, 2001), Russia would become a haven for hackers as the state tolerated the growth of the subculture (Delio, 2001). As the number of highly trained and unemployed youths increased, so did their desire to hack as a way to use their skills, socialise and access programs and tools not available freely within the USSR (Delio, 2001).

The hacker culture in Russia did not hold the negative connotations present in Western society due to, in part Soviet-era communist values and the view that there are more significant crimes of concern (Delio, 2001). While in the United States, hackers were seen as criminals due to their depiction in the media (Lee and Holt, 2017), in Russia, hackers were a common feature of society due to their presence in market stalls and the states non-intervention (Delio, 2001). Similar to the hacker subculture in other countries, the Russian hacker subculture involved forming an identity that revolved around skills and hacking activities and engaging with other hackers to form a sense of collectivism (Dremliuga, 2014; Lee and Holt, 2017). Arguably, this desire for a hacker identity likely resulted from young unemployed men within Russia experiencing a sense of social isolation and a desire a new outlet for entertainment, social stimulation, money and meaning (Lee and Holt, 2017). Through collectivism and social comradery that the subculture provided, hackers could exchange their knowledge and find justification for their illicit activities (Holt and Copes; Lee and Holt, 2017), providing a sense of fulfilment for Russian hackers.

The growth of the hacker subculture within Russia from the 1980s to the early 2000s formed the foundational environment where hacking within Russia was not only acceptable but idealised and seen as an acceptable lifestyle (Dremliuga, 2014; Dremliuga et al., 2020). Within the Russian hacker subculture, there are specific characteristics that set it apart from other subculture groups which have contributed to the appeal of RaaS to Russian hackers. The Russian hacker subculture has a strong emphasis on culture and collectivism; these characteristics specifically highlight the desire of the state to act as a protector and the need for state support (Dremliuga, 2014; Vershinin, 2004). Furthermore, as proposed by Holt et al. (2017), the Russian hacking subculture is built upon the Soviet culture to share resources to reduce their liability; therefore, the selling of ransomware aligns with the nature of the

Russian hacker subculture to mitigate risks. By enabling a hacker subculture to exist and flourish within Russia, the state allowed cybercrime to become permissible, which would make RaaS acceptable within Russia.

5.3 Russian Socioeconomics

While extensive research exists around the influence of socioeconomics on physical crimes, there has notably been limited analysis regarding the impact of socioeconomics on cybercrime rates, with the most notable research exploring the socioeconomics causes of cybercrime in Nigeria (Ibrahim, 2016). The section will examine the broader socioeconomic landscape within Russia, the role of unemployment and low wages within the I.T. sector, education rates, and wealth inequality has played in luring Russians toward RaaS. While socioeconomics contributed to the overall appeal of cybercrime, specific characteristics within Russian socioeconomics have promoted RaaS over other cybercrimes.

5.3.1 Employment

Gerber and Hout (1998) outlined that the USSR's collapse saw dramatic market reforms. These reforms saw a decline in living standards, and while this decline was predicted, academics, including Sachs (1992), anticipated growth soon after. However, this growth did not occur; instead, it would take until 2007, when Vladimir Putin was able to stabilise Russia's socioeconomic conditions (Shkolnikov, 2008) and decrease unemployment to 6.1%, compared to the 12.2% when Putin took power (Trading Economics, 2022), although, this number would be impacted the following year as a result of the Global Financial Crisis (Jacks et al., 2020). While Russia's unemployment rate has continued to decline since its high in the 1990s, this reduction was heavily influenced by the rapid increase in employment within the state-owned oil and gas sector (Shkolnikov, 2008; Vaisburd et al., 2016). Unemployment within the information technology sector is significant, with roughly half of Russian I.T specialists obtaining employment within Russia (Maurer, 2017).

The widespread unemployment within the I.T. sector is primarily due to Russia's lack of technological innovation, the heavy investment in STEM-based education (Dawisha, 2014; Gragido et al., 2013) and a non-existent software industry

(Dremliuga et al., 2020). With a lack of employment opportunities, those with I.T. skills have turned down the path of advertising their services on the dark web to earn an income (de Carbonnel, 2013; Maurer, 2017; Dremliuga et al., 2020), a path that is argued to "one of the few good jobs left" (Delio, 2001). Unemployment within the I.T. sector has lent itself to RaaS as the rise of the informal economy, and the commodification of ransomware has provided further opportunities for skilled I.T. professionals to sell their skills on the dark web in multiple ways and with the support of an organised criminal enterprise.

Additionally, those that are fortunate enough to find employment within the information technology sector often experience significant low wage returns, with the median salary for an I.T. professional in 2021 sitting at just under 10,000 USD (Statista, 2022), compared to Russia's Gross National Income (GNI) of 24,890 USD (Palvia et al., 2021). The low wage returns are arguably a result of Russia's the overall stagnations of wages and significant wealth inequality within the state (The Moscow Times, 2019). The lack of compensation within Russia's information technology sector results from multiple factors, including Russia's flexible labour market, a market used to prop up the state unemployment figures (Demmou and Wörgötteri, 2015) and the wage compression that began in the 1990s (Remington, 2018). To counterweigh the flexibility within the market, Russia experiences high wage inequality, informality within the labour market (Demmou and Wörgötteri, 2015), low productivity of labour (Vaisburd et al.,2016), and a lack of revenue-generating innovations within I.T. (Jacks et al., 2020).

Overall, the flexibility within the Russian labour market has arguably amplified the rise of the cybercrime gig economy (Shapiro, 2021), which like unemployment within the I.T. sector, has contributed to Russian I.T professionals turning to RaaS to reduce their financial risks. The appeal of high monetary rewards (Gragido, 2013) with little involvement from law enforcement (Burgess, 2022) in part compensates for the wage inequality, and the ability to create new and more challenging versions of ransomware (Check Point, 2022) counteracts the lack of innovation within the I.T. space.

5.3.2 Education

In addition to the role that employment has played in creating an environment ideal for the growth of RaaS, education within Russia has played a considerable part in creating a generation of skilled ransomware criminals. While previous research highlights the negative relationship between education and crime rates for physical crimes (Lochner, 2004; Lochner and Moretti, 2004), the opposite can be argued regarding cyber-based crimes. As outlined by Benjamin et al. (2016) and Park et al. (2019), there is a positive connection between RaaS and education due to the high level of technical skills required to conduct cyber-based crime and increase the returns. Russia in 2019 had one of the highest rates of tertiary education completions, with 63 per cent of the population holding a tertiary education, compared to the average of only 44 per cent for OECD countries (OECD, 2019b). Of the 63 per cent, 35 per cent completed a STEM-based undergraduate degree, and 25 per cent completed a STEM-based master's degree. These high rates of education, coupled with the instability within the labour market, contributed to forming the foundation of RaaS in Russia.

While it could be argued that the high education rates do not lend themselves to RaaS over other crimes, one central counterargument should be considered, the returns on RaaS. As suggested, cybercrimes require a greater understanding of returns and the economy of scale (Benjamin et al., 2016; Park et al., 2019). RaaS appeals to these highly educated Russians as it allows them to make a significant profit without involving additional illicit activities, such as online drug dealing (McGuire, 2018). Furthermore, RaaS is appealing due to the ability to tailor ransomware code to avoid Russian targets (Mohanta et al., 2018), reduces the risk of capture and thus appeals to the risk-averse educated Russian hacker. The educational environment within Russia created the perfect landscape for these highly educated cyber criminals to seek out not only cybercrime but highly profitable cybercrime in the form of RaaS. Lusthaus (2018) supports the argument that highly educated Russian are enticed by RaaS, shedding light on the highly professional Russian hackers who only care for "money, money, money" (pp: 36) and are therefore enticed by RaaS and its high profitability.

The connection between education, RaaS and Russia is additionally apparent when comparing Russia to other countries with high levels of cybercrime. The education

rate of China is significantly lower than in Russia, with less than 20 per cent of the adult population holding a tertiary degree (OECD, 2019a); however, a large portion of spam emails have been attributed to Chinese-based cybercriminals (McCombie et al., 2009). Additionally, Nigeria, where *yahooboys* and online scams are flourishing (Adeniran, 2011; Tade, 2016), has low education rates, with 10 per cent of the population holding a tertiary degree in 2011 (The World Bank, 2021). While rates of cybercrimes are significant in Russia, China and Nigeria, only Russia has the highest level of RaaS attribution.

While some academics may argue that this is a result of other socioeconomic factors such as unemployment, lack of social assistance (Adeniran, 2011) or even access to broadband (Park et al., 2019; Barker, 2017), the role that education plays in creating an environment where RaaS can flourish is irrefutable. With significantly higher rates of adults completing tertiary education, Russia is a breeding ground of highly educated and skilled individuals who use their skills to not only commit cybercrimes but RaaS, which can bring in significant profits with little to no risk in comparison to other cyber-based crimes such as other forms of malware.

5.3.3 Wealth Inequality

A final aspect of socioeconomics that has played a role in Russia's cultivation of RaaS is the hoarding of wealth by the Russian elites. The wealth gap creates an uneven playing field between different socioeconomic status levels (Mendoza, 2020), influencing an individual's starting point concerning employment and housing (Cysne, 2009; Smith et al., 2022). As indicated by Zhu and Lin (2019), the root causes of the wealth gap include political and social factors; within Russia, the leading factor is the institutional flaws within the market economy. The wealth inequality within Russia is significant, with just the top five hundred of Russia’s richest holding a combined wealth of $640 billion in 2020 (Sibley, 2022). Notably, while there is an ongoing trend of increased wealth inequality globally (Remington, 2018), Russia’s wealth gap has been an ongoing feature even during the USSR, with the Soviet top one per cent living well above the standard of the average citizen (Novokmet et al., 2018)

Russian oligarchs and the wealthy have utilised a plethora of techniques to hoard wealth, including exploiting government policy and loopholes within policy, colluding with government agents and manipulating the market (Zhu and Lin, 2019; Russell, 2018). Through these techniques, Russia's richest 10 per cent own 87 per cent of all of the nation's wealth (Walker, 2017). While hoarding wealth has had an evident impact on Russia's economic growth, it has had far-reaching social implications. Expanding on the Marxist explanation of crime, the dramatic wealth gap within Russia has led to an increase in resentment towards society from the underclass, which in turn increases the number of individuals turning to RaaS to cope with social disorganisation and negative emotions (Garg and Camp, 2015; Park et al., 2019; Zhu and Lin, 2019).

Furthermore, while the wealth gap and wage compression has contributed to individuals turning to RaaS to supplement their insufficient incomes, the wealth gap has contributed to the growth of RaaS in Russia as it has prohibited any meaningful reforms in policy from occurring. Through the abuse of their wealth and power, the Russian elite has sought to implement self-serving policies that function to increase their already significant wealth (Shkolnikov, 2008; Markus, 2017). These manipulations prevent the implementation of meaningful social change with Russia that would reduce the economic appeal of cybercrime and RaaS, such as social welfare and employment opportunities (Garg and Camp, 2015; Park et al., 2019).

This chapter examined the complex topic of the socio-technological influences that have contributed to the growth of RaaS in Russia. By utilising an approach that considers the sociological and technological impacts, a more holistic understanding of the role the environment and behaviour play in the adoption of ransomware is possible. This chapter highlighted the key role of Russia's technological history, socioeconomics, and organised crime history in contributing to the cultivation of RaaS in Russia.

Conclusions

Within the cyber landscape, no threat has grown the fastest and has been more damaging than ransomware (Grobman and Cerra, 2016). This research thesis set out to answer the question, how has the Russian state facilitated the growth of RaaS within Russia? Specifically, this thesis's purpose was to identify and examine the political and socio-technical factors that have contributed to the growth of RaaS within Russia to understand the state's role in the cultivation of RaaS in Russia. Furthermore, this research thesis utilised the political and socio-technical lens to examine Russia's cultivation of RaaS to enable a deeper analysis into the causes of RaaS beyond just the technological, but to allow a more holistic understanding of RaaS offending. Research findings indicated that since its adoption as a

cyberwarfare tool by the Russian state in 2017, the use of RaaS within Russia has seen significant growth with three key contributing pillars underpinning this rise: the political-criminal nexus, the deliberate involvement and purposeful non-intervention of the political elite and the inequality stemming from Russia's socio-technical landscape.

As this project argued, it is essential to view these three political and socio-technological factors in unison, giving a more holistic overview of the factors beyond just the technological that are contributing to the growth of cybercrimes including RaaS. While previous research regarding ransomware focused predominately on the technical influences that led to its growth, this research demonstrated the significant role that socio-technological influences have had on the rise of RaaS. Most distinctively, this research project identified that the growth of RaaS in Russia is a direct result of the permissive environment created by the Russian state. The cultivation of RaaS within Russia resulted from a legacy of corruption, ineffective cyber legislation, active cyber aggression, and a socio-technical landscape that benefitted the political elite.

6.1 The Political-criminal Nexus

As argued by Vaksberg (1991), corruption blurs the lines between the state and organised crime, and through their corrupt actions, the Russian state has become deliberately involved with organised cybercrime groups, including RaaS. This research project highlighted that the Russian state created a unique environment that has allowed RaaS to flourish due to its ongoing connection with organised crime, which would develop into a relationship with RaaS groups. Throughout the evolution of Russian-based ransomware and Russian organised crime, the state has played a continual influential role which due the political-criminal nexus and the benefits that the relationship provided to the political elites. Furthermore, the political-criminal nexus emphasised the significant role that Russia's corrupt landscape has played in the development of RaaS within the state with the nexus providing cybercriminals an unprecedented level of protection.

6.2 Deliberate Involvement and Purposeful Non-intervention

The lack of efficient laws and policies regarding cybercrime (Dremliuga et al., 2020: Kadlecová, 2015) within Russia further emphasised the state's purposeful non-intervention in preventing the growth of RaaS. Russian RaaS groups understood and manipulated Russia's cybercrime legislation to conduct activities that would allow the state to be a soft benefactor to their activities. As demonstrated by the lack of any effective legal recourse against RaaS groups, the Kremlin is permissive to RaaS and have failed to implement any policy that would stem their growth. So long as RaaS groups support the state's nationalistic agenda, their activities are supported by the Kremlin.

Notably, the shift from the Russian state being a soft benefactor of RaaS to an active participant would further contribute to the growth of RaaS within the state. The Russian state's participation in cyberwarfare, most notably through their use of ransomware during the 2017 NotPetya, distorted the line between the state and organised ransomware groups. While arguably the involvement of the Russian state in criminal activities is not a new concept (McCarthy-Jones and Turner, 2021), the state's active participation in RaaS underscored once again to organised cybercrime groups that RaaS was permitted so long as it supported the goals of the Kremlin.

6.3 Socio-technical Inequality

Research shows that high social inequality results in higher organised crime development (Battisti et al., 2020). The Russian state purposefully created a country with high inequality through their rampant corruption, the raiding of social budgets by the political elite (Dawisha, 2014) and its non-intervention in reducing the wealth gap. These high rates of inequality, combined with data that indicates that eighty per cent of cybercrime results from some form of organised criminal activity (Broadhurst et al., 2013; McGuire, 2012), the Russian state created an environment receptive to RaaS as highly educated Russians unable to find profitable employment turned to cybercrime.

Beyond the socioeconomic influences that allowed RaaS to flourish in Russia, the technological history of the nation would also play a role. As the Russian state pushed for the expansion of STEM education to match that of the United States, the

state failed to create employment opportunities for these skilled professionals. Disillusioned by the state, these individuals would turn to the hacker subculture to find social support and profit through illegal activities. Through creating an environment filled with skilled hackers, the Russian state once again cultivated a landscape where cybercrimes like RaaS could grow.

6.4 Future Research

During this research project several questions emerged that were not answered due to the scope of the project, the most notable question being the political and sociological influences contributing to the growth of cybercrime globally. While this research answered the question of the Russian state's role in cultivating RaaS, by evaluating the political and social influences on global cybercrime a greater holistic understanding of cybercrime is achievable. Through this additional research, cybersecurity professionals could further anticipate trends within the cybersecurity landscape to identify new threats. Additional research should question the Russian state's role in cultivating other forms of cybercrime, including phishing and hacking. This future research may assist in identifying additional trends within Russia's political and socio-technological landscape that elucidate the influence of the Russian state on the criminal underworld. While there are still gaps within our knowledge of cybercrimes, this research project highlighted that while cybercrimes are viewed as a technological problem, the solutions require a political and sociological understanding. This research project is the first step in understanding these solutions.

References

Adeniran A (2011) Café Culture and Heresy of Yahooboyism in Nigeria. In: Jaishankar K (ed) *Cyber Criminology. Exploring Internet Crimes and Criminal Behaviour*. Florida: CRC Press, pp. 3-12.

Ahn G, Doupe A, Zhao Z and Liao K (2017) Ransomware and cryptocurrency: partners in crime. In: Holt T (eds) *Cybercrime Through an Interdisciplinary Lens*. New York: Routledge, pp. 105-126.

Albini J, Rogers R, Shabalin V, Kutushev V, Moiseev V and Anderon J (1995) Russian Organized Crime: Its History, Structure and Function. *Journal of Contemporary Criminal Justice* 11(4): pp. 213-243.

Alexander C (1985) Playing Computer Catch-Up. Time. Available at: http://content.time.com/time/subscriber/article/0,33009,966203-1,00.html (accessed 3 July 2022).

Alexander C and Daniel H (2020) Price Discovery in Bitcoin: The Impact of unregulated markets. *Journal of Financial Stability* 50(2020): pp. 100775-.

Åslund A (2017) Russia's Neo-Feudal Capitalism. Available at: https://www.project-syndicate.org/commentary/russia-neofeudal-capitalism-putin-by-anders-aslund-2017-04 (accessed 25 May 2022).

Australian Cyber Security Centre (2021) ACSC Annual Cyber Threat Report. 1 July 2020 to 30 June 2021. Report, Australia, September.

Australian Cyber Security Centre (2022a) 2021-010: ACSC Ransomware Profile – Conti. Report, Australian Signals Directorate, Australia, March.

Australian Cyber Security Centre (2022b) ACSC Ransomware Profile – ALPHV (aka BlackCat). Available at: https://www.cyber.gov.au/sites/default/files/2022-04/ACSC%20Ransomware%20Profile%20Alphv%20%2814%20April%202022%29%20-%20PDF.pdf (accessed 9 May 2022).

Australian Cyber Security Centre (2022c) Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure. Available at: https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure (accessed 22 June 2022).

Avertium (2022) BlackCat Ransomware and Triple Extortion. Available at: https://www.avertium.com/resources/threat-reports/blackcat-ransomware-and-triple-extortion (accessed 30 April 2022).

Bakarv M (2017) The Russian Reversal. From Developed to Emerging IT. *IT Professional* 19(3): pp. 11-13.

Baker K (2022) Ransomware as a Service (RaaS) Explained. Available at: https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/ (accessed 8 April).

Baldwin K and Dehghantanha A (2018) Leveraging Support Vector Machine for Opcode Density Based Detection of Crypto-Ransomware. In: Dehghantanha A, Conti M and Dargahi T (eds) *Cyber Threat Intelligence.* Switzerland: Springer, pp. 107-136.

Baraniuk C (2016) Why the forgotten Soviet internet was doomed from the start. BBC. Available at: https://www.bbc.com/future/article/20161026-why-the-forgotten-soviet-internet-was-doomed-from-the-start (accessed 2 July 2022).

Bargent J (2013) Why Has the Italian Mafia Returned to Colombia? InSight Crime. Available at: https://insightcrime.org/news/analysis/why-has-the-italian-mafia-returned-to-colombia/ (accessed 23 September 2022).

Barker S (2017) Need for speed: The connection between faster internet and cyber attacks. Available at: https://securitybrief.co.nz/story/need-speed-connection-between-faster-internet-and-cyber-attacks (accessed 25 May 2022).

Battisti M, Bernardo G, Konstantinidi A, Kourtellos A and Lavezzi A (2020). Socio-Economic Inequalities and Organized Crime: An Empirical Analysis. In: Weisburd D, Savona E, Hasisi B and Calderoni F (eds) *Understanding Recruitment to Organized Crime and Terrorism*. Switzerland: Springer, pp: 205-240.

Beck A and Lee R (2022) Attitudes to Corruption amongst Russian Police Officers and Trainees. *Crime, Law and Social Change*, 38(4): pp. 357–7.

Bederna Z and Szadeczky T (2019) Cyber espionage through Botnets. *Security Journal* 33: pp. 43-62.

Belton C (2020) *Putin's People. How the KGB Took Back Russia and then Took on the West*. London: Harper Collins.

Benjamin V, Zhang B, Nunamaker Jr. J and Chen H (2016) Examining Hacker Participation Length in Cybercriminal Internet-Relay-Chat Communities, *Journal of Management Information Systems*, 33(2): pp. 482-510.

Bennetts M (2018) Why Putin's Corruption Crackdown May Be a Pre-Election Show. Newsweek. Available at: https://www.newsweek.com/putin-corruption-crackdown-pre-election-show-830704 (accessed 1 July 2022).

Bernard A (2020) Chinese cyber criminals are getting more organized and dangerous. Available at: https://www.techrepublic.com/article/chinese-cyber-criminals-are-getting-more-organized-and-dangerous/ (accessed 3 October 2022).

Birch K (2021) US and Canada among countries most attacked by ransomware. Available at: https://businesschief.com/technology-and-ai/us-and-canada-among-countries-most-attacked-ransomware (accessed 27 September 2022).

BlackFrog (2022) Beyond the Ransom: The True Cost of Ransomware Attacks. Available at: https://www.blackfog.com/the-true-cost-of-ransomware-attacks/ (accessed 16 September 2022).

Blue V (2013) CryptoLocker's crimewave: A trail of millions in laundered Bitcoin. ZDNet. Available at: https://www.zdnet.com/article/cryptolockers-crimewave-a-trail-of-millions-in-laundered-bitcoin/ (accessed 18 September 2022).

Boll-Stiftung H and Schonenberg R (2013) *Transnational Organized Crime. Analyses of a Global Challenge to Democracy*. Bielefeld: Transcript.

Bourguignon F (1999) Crime as a Social Cost of Poverty and Inequality: A Review Focusing on Developing Countries. *Revista Desarrollo y Sociedad*, 44: pp. 61-99.

Boylan S (1995) Organized Crime and Corruption in Russia: Implications for U.S. and International Law. Fordham International Law Journal, 19(5): pp. 1999-2027.

Braaten C and Vaughn M (2021) Convenience Theory of Cryptocurrency Crime: A Content Analysis of U.S. Federal Court Decisions, *Deviant Behavior* 42(8): pp. 958-978.

Bright D and Leiva A (2021) Transnational Criminal Networks. In: Allum F and Gilmour S (eds) *The Routledge Handbook of Transnational Organized Crime*. London: Routledge, pp. 35-50.

Briscoe I and Kalkman P (2016) The new criminal powers. The spread of illicit links to politics across the world and how it can be tackled. Report, Clingendel, Netherlands, January.

Broadhurst R, Grabosky P, Alazab M, Bouhours B, Chon S and Da C (2013) Crime in cyberspace: Offenders and the role of organized crime groups. *SSRN Electronic Journal* pp: 2-42.

Broadhurst R, Grabosky P, Alazab M and Chon S (2014) Organizations and Cyber Crime: An Analysis of the Nature of Groups engaged in Cyber Crime. *International Journal of Cyber Criminology* 8(1): pp. 1-20.

Buil-Gil D and Saldaña-Taboada P (2021): Offending Concentration on the Internet: An Exploratory Analysis of Bitcoin-related Cybercrime. *Deviant Behavior*: pp. 1-18

Bush J (2004) Russian science still tops. Australian Financial Review. Available at: https://www.afr.com/policy/health-and-education/russian-science-still-tops-20041101-jk9l8 (accessed 3 October 2022).

Canales K (2021) Experts say Russia gives hackers a 'tacit blessing' to attack foreign nations — as long as they don't target Russia or its allies. Insider. Available at: https://www.businessinsider.com/russia-safe-haven-hackers-cybercriminals-putin-ransomeware-blessing-2021-6 (accessed 27 September 2022).

Casciani D (2019) Zain Qaiser: Student jailed for blackmailing porn users worldwide. BBC. Available at: https://www.bbc.com/news/uk-47800378 (accessed 1 May 2022).

Check Point (2022) How the evolution of ransomware has changed the threat landscape. Available at: https://blog.checkpoint.com/2022/05/11/how-the-evolution-of-ransomware-changed-the-threat-landscape/ (accessed 5 June 2022).

Cheloukhine S (2008) The roots of Russian organized crime: From old-fashioned professionals to the organized criminal groups of today. *Crime, Law and Social Change* 50(4-5): pp. 353-374.

Cheloukhine S and Haberfeld M (2011) *Russian Organized Corruption Networks and their International Trajectories*. London: Springer.

Cheloukhine S, Khan V and Kalkayeva N (2021) Transnational organized crime and corruption in Russia: its origin and current development. In: Allum F and Gilmour S (eds) *The Routledge Handbook of Transnational Organized Crime*. London: Routledge, pp. 105-127.

Chêne M (2008) Organised crime and corruption. Available at: https://www.u4.no/publications/organised-crime-and-corruption.pdf (accessed 21 July 2022).

Chislova O and Sokolova M (2021) Cybersecurity in Russia. *International Cybersecurity Law Review* 2(2): pp. 245-251.

Choi K (2015) *Cybercriminology and digital investigations*. El Paso: LFB Scholarly Publishing.

Choo R and Grabosky P (2013) Cyber Crime. In: Paoli L (ed) *The Oxford Handbook of Organized Crime.* London: Oxford University Press, pp. 483-499.

Coker J (2022) Healthcare and Education Sectors Most Susceptible to Cyber Incidents. Info Security Magazine. Available at: https://www.infosecurity-magazine.com/news/healthcare-education-cyber/ (accessed 27 September 2022).

Conti M, Gangwal A, and Ruj S (2018a) On the economic significance of ransomware campaigns: A Bitcoin transactions perspective. *Computers & Security* 79: pp. 162-189.

Conti M, Kumar S, Lal C and Ruj S (2018b) A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys and Tutorials* 20(4): pp. 3416-3452.

CrowdStrike (2021a) 2021 Global Threat Report. Report, CrowdStrike, USA.

CrowdStrike (2021b) History of Ransomware. Available at: https://www.crowdstrike.com/cybersecurity-101/ransomware/history-of-ransomware/ (accessed 22 April 2022).

CrowdStrike (2021c) The Evolution of Ransomware: How to Protect Against New Adversary Trends and Methods. Report, CrowdStrike, USA.

Cusack B and Ward G (2018) Points of failure in the ransomware electronic business model. In: *AMCIS 2018 Proceedings*, 16 September 2018.

Cyber Threat Alliance (2018) Lucrative Ransomware Attacks: Analysis of the CryptoWall Version 3 Threat. Report, Cyber Threat Alliance, February.

Cybereason (2021) Cybereason vs. DarkSide Ransomware. Available at: https://www.cybereason.com/blog/research/cybereason-vs-darkside-ransomware (accessed 29 April 2022).

Cysne R (2009) On the Positive Correlation Between Income Inequality and Unemployment. *The Review of Economics and Statistics* 91(1): pp. 218-226

Davidson J (2022) How the spoils of cyberattacks are funding Russia's invasion. Australian Financial Review. Available at: https://www.afr.com/technology/business-cyber-ransoms-funding-russia-s-ukraine-war-20220422-p5afcz (accessed 27 September 2022).

Davies E (2019) Is cryptocurrency helping Russia to avoid US sanctions? Available at: https://finance.yahoo.com/news/cryptocurrency-helping-russia-avoid-us-180004372.html (accessed 18 September 2022).

Dawisha K (2014) *Putin's Kleptocracy*. New York: Simon and Schuster.

De Carbonnel A (2013) Ex-Soviet hackers play outsized role in cyber crime world. Available at: https://www.reuters.com/article/uk-russia-cybercrime-idUKBRE97L0TN20130822 (accessed 5 June 2022).

Dean G, Fahsing, I and Gottschalk P (2010) Criminal Enterprises, Markets and Industries. In: *Organized Crime: Policing Illegal Business Entrepreneurialism*. Oxford University Press: New York, pp. 19-40.

Dean J (2020) Neofeudalism: The End of Capitalism? Available at: https://lareviewofbooks.org/article/neofeudalism-the-end-of-capitalism/ (accessed 23 September 2022).

Delio M (2001) Inside Russia's Hacking Culture. Wired. Available at: https://www.wired.com/2001/03/inside-russias-hacking-culture/ (accessed 16 June 2022).

Demmou L and Wörgötter A (2015) Boosting Productivity in Russia: Skills, Education and Innovation. *OECD Economics Department Working Papers No 1189*. Paris: OECD Publishing.

Department of Homeland Security (2017) Indicators Associated with WannaCry Ransomware. Available at: https://www.cisa.gov/uscert/ncas/alerts/TA17-132A (accessed 24 April 2022).

DiMaggio J (2021) Nation State Ransomware. Report, Analyst1, USA, August.

Dremliuga R, Dremliuga O and Kuznetsov P (2020) Combating the Threats of Cybercrimes in Russia. Evolution of the Cybercrime Laws and Social Concern. *Communist and Post-Communist Studies*, 53(3): pp. 123-136.

Dresen F (2022) The Growth of Russia's IT Outsourcing Industry: The Beginning of Russian Economic Diversification? Available at: https://www.wilsoncenter.org/publication/the-growth-russias-it-outsourcing-industry-the-beginning-russian-economic (accessed 2 July 2022).

Eichten M (2010) The Computer Fraud and Abuse Act—A Survey of Recent Cases. *The Business Lawyer* 66(1): pp. 231-236.

Europol (2021) Internet Organised Crime Threat Assessment (IOCTA) 2021. Report for Office of European Union, Luxembourg.

Faife C (2022) A ransomware group paid the price for backing Russia. Available at: https://www.theverge.com/2022/2/28/22955246/conti-ransomware-russia-ukraine-chat-logs-leaked (access 5 June 2022).

Falco G (2022) Who is Attacking Us? In: Falco G and Rosenbach E (eds) *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. New York: Oxford University Press, pp. 16-40.

Feeley B and Hartley B (2019) “Sin”-ful SPIDERS: WIZARD SPIDER and LUNAR SPIDER Sharing the Same Web. Available at: https://www.crowdstrike.com/blog/sin-ful-spiders-wizard-spider-and-lunar-spider-sharing-the-same-web/ (accessed 30 June 2022).

Fenghi F (2020) *It Will Be Fun and Terrifying: Nationalism and Protest in Post-Soviet Russia*. Madison: University of Wisconsin Press.

Fisher, D (2015) FBI Says Cryptowall Cost Victims $18 Million Since 2014. Available at: https://threatpost.com/fbi-says-cryptowall-cost-victims-18-million-since-2014/113432/ (accessed 18 September 2022).

Frye T (2021) *Weak Strongman: The Limits of Power in Putin's Russia*. New Jersey: Princeton University Press.

Galeotti M (1998) The Mafia and the New Russia. *Australian Journal of Politics and History* 44(3): pp. 415-429.

Galeotti M (2004) The Russian 'Mafiya': Consolidation and Globalisation. *Global Crime* 6(1): pp. 54-69.

Galeotti M (2009) Profit and loss - Russian crime network faces business strain. *Janes Intelligence Review* 21(6): pp. 44-47.

Galeotti M (2017) *Crimintern: How the Kremlin uses Russia's Criminal Networks in Europe*. Report for European Council on Foreign Relations. Report no. ECFR/208, April. London.

Galeotti M (2018a) Gangster's paradise: how organised crime took over Russia. The Guardian. Available at: https://www.theguardian.com/news/2018/mar/23/how-organised-crime-took-over-russia-vory-super-mafia (accessed 21 July 2022).

Galeotti M (2018b) *The Vory. Russia's Super Mafia*. New Haven: Yale University Press.

Garg V and Camp L (2015) Why Cybercrime? *SIGCAS Computers & Society* 45(2): pp. 20-28.

Gazet A (2010) Comparative analysis of various ransomware virii. *J Comput Virol* 6: pp. 77-90.

Gerber T and Hout M (1998) More Shock Than Therapy: Market Transition, Employment, and Income in Russia, 1991-1995. *American Journal of Sociology* 104(1): pp. 1-50.

Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A and Aylin P (2019) A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digital Medicine* 2019(98): pp. 1-7.

Giri B and Jyoti N (2006) The Emergence of Ransomware. Report for McAfee AVERT, India.

Glenny M (2008) *McMafia. A Journey Through the Global Criminal Underworld*. New York: Alfred A. Knope.

Global Security (2022) Federal Security Service (FSB). Available at: https://www.globalsecurity.org/intell/world/russia/fsb.htm (accessed 1 October 2022).

Godson R (2003) The Political-Criminal Nexus and Global Security. In: Godson R (ed) *Menace to Society*. *Political-Criminal Collaboration Around the World*. USA: Transaction Publishers, pp. 1-27.

Gomez M (2021) Breaking the Myth of Cyber Doom: Securitization and Normalization of Novel Threats. *International Studies Quarterly* 65(4): pp. 1137-1150.

Gottschalk P (2010) Entrepreneurship in organised crime. *Entrepreneurship and Small Business* 9(3): pp. 295-307.

Gottschalk P (2017a) Convenience in White-Collar Crime: Introducing a Core Concept. *Deviant Behavior* 38: pp. 605-619.

Gottschalk P (2017b) *Understanding White Collar Crime. A Convenience Perspective*. Boca Raton: CRC Press.

Grabosky P (2015) Organized Cybercrime and National Security. In: Smith R, Cheung R and Lau L (eds.) *Cybercrime Risks and Responses. Eastern and Western Perspectives*. New York: Palgrave Macmillan, pp. 67-80.

Grabosky P (2016) *Cybercrime*. New York: Oxford University Press.

Gragido W, Molina D, Pirc J and Selby N (2013) *Blackhatonomics an inside look at the economics of cybercrime*. Amsterdam: Syngress.

Greenberg A (2013) Follow the bitcoins: how we got busted buying drugs on the silk road's black market. Forbes. Available at: https://www.forbes.com/sites/andygreenberg/2013/09/05/follow-the-bitcoins-how-we-got-busted-buying-drugs-on-silk-roads-black-market/?sh=5f6420a1adf7 (access 22 April 2022).

Greenberg A (2018) The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. Available at: https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/ (accessed 29 April 2022).

Greenberg A (2019) *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers*. Doubleday, New York.

Grimes R (2021) *Ransomware Protection Playbook*. New Jersey: John Wiley & Sons.

Grobman S and Cerra A (2016) *The Second Economy: The Race for Trust, Treasure and Time in the Cybersecurity War*. Berkeley: Apress.

Groot J (2022) A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time. Available at: https://digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time (accessed 30 September 2022).

Hakala J and Melnychuk J (2021) Russia's Strategy in Cyberspace. Report for NATO Strategic Communications Centre of Excellence. Report no. 978-9934-564-90-1, June. Latvia

Hale H (2016) How nationalism and machine politics mix in Russia. In: Kolstø P and Blakkisrud H (eds) *The New Russian Nationalism*. Edinburgh: Edinburgh University Press, pp. 221-248.

Harding L (2020) Navalny says Russian officer admits putting poison in underwear. The Guardian. Available at: https://www.theguardian.com/world/2020/dec/21/navalny-russian-agent-novichok-death-plot (accessed 1 October 2022).

Hassan N (2019) *Ransomware revealed*. Berkeley: Apress.

Higbee A (2018) The role of crypto-currency in cybercrime. *Computer Fraud & Security* 2018(7): pp. 13-17.

Hill J (2022) BlackCat Ransomware (ALPHV). Available at: https://www.varonis.com/blog/blackcat-ransomware (accessed 1 May 2022).

Hoffman D (2000) Putin's Career Rooted in Russia's KGB. The Washington Post. Available at: https://www.washingtonpost.com/wp-srv/inatl/longterm/russiagov/putin.htm (accessed 22 June 2022).

Holmes L (2008) Corruption and Organised Crime in Putin's Russia. Europe-Asia Studies 60(6): pp. 1011-1031.

Holt T and Copes H (2010) Transferring subcultural knowledge on-line: Practices and beliefs of persistent digital pirates. *Deviant Behavior*, 31(7): pp. 625–654.

Holt T, Freilich J and Chermak S (2017) Exploring the Subculture of Ideologically Motivated Cyber-Attackers. *Journal of Contemporary Criminal Justice* 33(3): pp. 212-233.

Homayoun S, Ahmadzadeh M, Hashemi S, Dehghantanha A and Khayami R (2018) BotShark: A Deep Learning Approach for Botnet Traffic Detection. In: Dehghantanha

A, Conti M and Dargahi T (eds) *Cyber Threat Intelligence.* Switzerland: Springer, 137-154.

Horsley E (2019) State-Sponsored Ransomware Through the Lens of Maritime Privacy. *The Georgia Journal of International and Comparative Law* 47(3): pp. 669-

House of Representatives Standing Committee on Communications (2010) Hackers, Fraudsters and Botnets. Tackling the problem of cyber crime. Report, Inquiry into Cyber Crime, Canberra, June.

Hughes D and Denisova T (2001) The Transnational Political Criminal Nexus of Trafficking in Women from Ukraine. *Trends in Organized Crime* 6(3-4): pp. 43-67.

Hutchby I (2003) Affordances and the Analysis of Technologically Mediated Interaction: A Response to Brian Rappert. *Sociology* 37: pp. 581-589

Ibrahim S (2016) Causes of socioeconomic cybercrime in Nigeria. In: *IEEE International Conference on Cybercrime and Computer Forensic*, Vancouver, Canada, pp. 1-9. IEEE Publishing.

Idris I (2022) *Corruption, crime and conflict in eastern Ukraine*. Report, University of Birmingham, UK, May.

INTERPOL (2022) Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams. Available at: https://www.interpol.int/en/News-and-Events/News/2022/Hundreds-arrested-and-millions-seized-in-global-INTERPOL-operation-against-social-engineering-scams (accessed 24 September 2022).

Introna L and Pecis L (2019) Bitcoin as a mediating technology of organization. In: Beyes T, Holt R and Pias C (eds) *The Oxford Handbook of Media, Technology, and Organization Studies*. London: Oxford University Press, pp. 43-53.

Jacks T, Kazantsev N and Serenko A (2020) Information Technology Issues in Russia. In: Palvia P, Ghosh J, Jacks T, Serenko A and Turan A (eds) *The World IT Project. Global Issues in Information Technology*. Singapore: World Scientific Publishing, pp. 383-392.

Jacobs J (2020) The Rise and Fall of Organized Crime in the United States. *Crime and Justice* 49: pp. 17-67.

Jarvis K (2013) CryptoLocker Ransomware. Available at: https://papers.vx-underground.org/papers/Malware%20Defense/Malware%20Analysis/2013-12-18%20-%20CryptoLocker%20Ransomware.pdf (accessed 12 August 2022).

Joint Cybersecurity Advisory (2022) *2021 Trends Show Increased Globalized Threat of Ransomware*. Report for Joint Cybersecurity Advisory, report no. AA22-040A, 9 February.

Kadlecová L (2015) Russian-speaking Cyber Crime: Reasons behind Its Success. *The European Review of Organised* Crime, 2(2): pp. 104-121.

Karlovsky B (2014) Hackers hold almost 20,000 Australians to ransom using CryptoWall. Available at: https://www.arnnet.com.au/article/555511/hackers-hold-almost-20-000-australians-ransom-using-cryptowall/ (accessed 18 September 2022).

Karstedt S (2014) Organizing Crime: The State as Agent. In: Paoli L (ed) *The Oxford Handbook of Organized Crime*. London: Oxford University Press, pp. 303-320.

Kawamoto D (2006) Trojan Cryzip extorts decryption fee. ZDNet. Available at: https://www.zdnet.com/article/trojan-cryzip-extorts-decryption-fee/ (accessed 12 April 2022).

Kaylan M (2014) Kremlin Values: Putin's Strategic Conservatism. *World Affairs*, 177(1): pp. 9-17

Kerner S (2022) Ransomware trends, statistics and facts in 2022. Available at: https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts (accessed 30 September 2022).

Kerns Q, Payne B and Abegaz T (2022) Double-Extortion Ransomware: A Technical Analysis of Maze Ransomware. In: Arai K (ed) *Proceedings of Future Technologies Conference (FTC) 2021, Volume 3*. Switzerland: Springer, pp. 82-94.

Kerr S (1991) Educational Reform and Technological Change: Computing Literacy in the Soviet Union. Comparative Education Review, 35(2): pp. 222-254.

Kethineni S, Cao Y and Dodge C (2018) Use of Bitcoin in Darknet Markets: Examining Facilitative Factors on Bitcoin-Related Crimes. *American Journal of Criminal Justice* 43(2): pp. 141-157.

Knowbe4 (2022) CryptoWall Ransomware. Available at: https://www.knowbe4.com/cryptowall (accessed 27 September 2022).

Kost E (2022) What is Ransomware as a Service (RaaS)? The Dangerous Threat to World Security. Available at: https://www.upguard.com/blog/what-is-ransomware-as-a-service (accessed 29 April 2022).

Kramer A (2016) How Russia Recruited Elite Hackers for Its Cyberwar. The New York Times. Available at: https://www.nytimes.com/2016/12/29/world/europe/how-russia-recruited-elite-hackers-for-its-cyberwar.html (accessed 27 September 2022).

Krebs B (2021a) Arrest, Seizures Tied to Netwalker Ransomware. Available at: https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware/ (accessed 30 April 2022).

Krebs B (2021b) A Closer Look at the DarkSide Ransomware Gang. Available at: https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/ (accessed 29 April 2022).

Krebs B (2021c) Ransomware Gangs and the Name Game Distraction. Available at: https://krebsonsecurity.com/2021/08/ransomware-gangs-and-the-name-game-distraction/ (accessed 1 May 2022).

Krebs B (2021d) Try this one weird trick Russian hackers hate. Available at: https://krebsonsecurity.com/2021/05/try-this-one-weird-trick-russian-hackers-hate/ (accessed 21 April 2022).

Kundaliya D (2019) Russia's new cyber laws will fuel online crime, claims report. Available at: https://www.computing.co.uk/news/3080270/russia-cyber-crime (accessed 29 June 2022).

Kuttner R and Stone K (2020) The Rise of Neo-Feudalism. Available at: https://prospect.org/economy/rise-of-neo-feudalism/ (accessed 23 September 2022).

Lai B (2022) The threat of ransomware. Available at: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook47p/ThreatRansomware (accessed 18 September 2022).

Lally C (2021) Wizard Spider profile: Suspected gang behind HSE attack is part of world's first cyber-cartel. The Irish Times. Available at: https://www.irishtimes.com/news/crime-and-law/wizard-spider-profile-suspected-gang-behind-hse-attack-is-part-of-world-s-first-cyber-cartel-1.4568806 (accessed 29 March 2022).

Lanskoy M and Myles-Primakof D (2018) The Rise of Kleptocracy: Power and Plunder in Putin's Russia. *Journal of Democracy* 29(1): pp. 76-85.

Latypova E, Nechaeva E, Gilmanov E and Aleksandrova N (2019) Infringements on Digital Information: Modern State of the Problem. *SHS Web Conferences* 62: pp. 1-5

Lavorgna A (2019) Cyber-organised crime. A case of moral panic? *Trends in Organized Crime* 22(4): pp. 357-374.

Lee H and Choi K (2021) Interrelationship between Bitcoin, Ransomware, and Terrorist Activities: Criminal Opportunity Assessment via Cyber-Routine Activities Theoretical Framework. *Victims & Offenders* 16(3): pp. 363-384.

Lee B and Holt T (2017) The Hacker Subculture. In: Brown S and Sefiha O (eds) *Routledge Handbook on Deviance*. New York: Routledge, pp. 299-308.

Lepido D, Gallagher R and Brambilla A (2022) Suspected Russian Ransomware Group Hacks Italian Energy Agency. Available at: https://www.bloomberg.com/news/articles/2022-09-02/suspected-russian-ransomware-group-hacks-italian-energy-agency (accessed 24 September 2022).

Leukfeldt R, Lavorgna A and Kleemans E (2017) Organised Cybercrime or Cybercrime that is Organised? An Assessment of the Conceptualisation of Financial Cybercrime as Organised Crime. *European Journal on Criminal Policy and Research* 23(3): pp. 287-300.

Lewis J (2022) A Dangerous Moment for Russian Cybercrime May Get Worse. Available at: https://www.barrons.com/articles/a-dangerous-moment-for-russian-cybercrime-may-get-worse-51644936090 (accessed 14 July 2022).

Liska A and Gallo T (2016) *Ransomware*. California: O'Reilly.

Lochner L (2004) Education, work, and crime: A human capital approach. *International Economic Review* 45(3): pp. 811–843.

Lochner L and Moretti E (2004) The effect of education on crime: Evidence from prison inmates, arrest, and self-reports. *American Economic Review* 94(1): pp. 155–189.

Lusthaus J (2018) Industry of Anonymity: Inside the Business of Cybercrime. USA: Harvard University Press.

Lyngaas S (2021) Russian state-backed hackers having greater success at breaching foreign government targets, Microsoft says. CNN. Available at: https://edition.cnn.com/2021/10/07/politics/russian-hackers-microsoft-report/index.html (accessed 1 October 2022).

March L (2012) 'Nationalism for Export? The Domestic and Foreign Policy Implications of the New "Russian Idea"', *Europe-Asia Studies*, 64(3): pp. 401-425

Marine F (2006) The effects of organized crime on legitimate businesses. *Journal of Financial Crime* 13(2): pp. 214-234.

Marks J (2022) Hopes of Russian help on ransomware are officially dead. The Washington Post. Available at: https://www.washingtonpost.com/politics/2022/06/01/hopes-russian-help-ransomware-are-officially-dead/ (accessed 22 June 2022).

Markus A (2017) The Atlas That Has Not Shrugged: Why Russia's Oligarchs are an Unlikely Force for Change. *Journal of the American Academy of Arts & Sciences* 146(2): pp. 101-112

Maurer T (2017) *Cyber Mercenaries. The State, Hackers, and Power*. Cambridge: Cambridge University Press.

Mauro L and Carmeci C (2007) A Poverty Trap of Crime and Unemployment. *Review of Development Economics* 11(3): pp. 450-465.

McCarthy-Jones A and Turner M (2021) What is a "Mafia State" and how is one created? *Policy Studies*: pp. 1-21.

McCombie S, Pieprzyk J and Watters P (2009) Cybercrime attribution: an Eastern European case study. In: *Proceedings of the 7th Australian Digital Forensics Conference* (ed. Cook D, Valli C, and Woodward A) Perth, Australia, pp. 41-51.

McGuire M (2012) *Organised Crime in the Digital Age*. Report, John Grieve Centre for Policing and Security, UK, March.

McGuire M (2018) *Into the Web of Profit. Understanding the Growth of the Cybercrime Economy.* Report for Bromium Inc, April. California.

Meduza (2018) 'It's our time to serve the Motherland' How Russia's war in Georgia sparked Moscow's modern-day recruitment of criminal hackers. Available at: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland (accessed 30 June 2022).

Meland P, Bayoumy Y and Sindre G (2020) The Ransomware-as-a-Service economy within the darknet. *Compusters & Science* 92: 1-9

Mendoza T (2020) How Does Socioeconomic Inequality Affect Social Class, Especially for People of Color? Available at: https://www.bu.edu/articles/2020/how-does-socioeconomic-inequality-affect-social-class-for-people-of-color/ (accessed 9 June 2022).

Millar S (2000) Sex gangs sell prostitutes over the internet. The Guardian. Available at: https://theguardian.com/technology/2000/jul/16/internetnews.theobserver1 (accessed 30 September 2022).

MITRE ATT&CK (2021) APT28. Available at: https://attack.mitre.org/versions/v10/groups/G0007/ (accessed 2 September 2022).

Mohanta A, Hadad M and Velmurugan K (2018) Preventing ransomware: understand, prevent, and remediate ransomware attacks. Birmingham: PACKT Publishing.

Mujezinovic D (2021) AIDS Trojan: The Story Behind the First Ever Ransomware Attack. Available at: https://www.makeuseof.com/aids-trojan-the-first-ransomware-attack-in-history/ (accessed 27 September 2022).

Nadir I and Bakhshi T (2018) Contemporary Cybercrime: A Taxonomy of Ransomware Threats & Mitigation Techniques. In: *International Conference on Computing, Mathematics and Engineering Technologies*, Sukkur, Pakistan, pp. 1-7.

Naím M (2012) Mafia States: Organized Crime Takes Office. *Foreign Affairs*, 91(3): pp. 110-111.

National Cyber Security Centre (2018) Reckless campaign of cyber attacks by Russian military intelligence service exposed. Available at: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed (accessed 24 June 2022).

Nikforov A (1993) Organized Crime in the West and in the Former USSR: An Attempted Comparison. *International Journal of Offender Therapy and Comparative Criminology* 37(1): pp. 5-15.

Nikolskaya P and Korsunskaya D (2017) Russian ex-minister Ulyukayev jailed for eight years over $2 million bribe. Available at: https://www.reuters.com/article/us-russia-ulyukayev-verdict-idUSKBN1E90SN (access 1 July 2022).

Novokmet F, Piketty T and Zucman G (2018) From Soviets to oligarchs: inequality and property in Russia 1905-2016. *Journal of Economic Inequality* 16(2): pp. 189-222.

OECD (2019a) Education at a Glance 2019: People's Republic of China. Available at: https://www.oecd-ilibrary.org/docserver/7c9859c1-en.pdf?expires=1653366595&id=id&accname=guest&checksum=8690A1A358F3564E094A1FEF15587DF6 (accessed 24 May 2022).

OECD (2019b) Education at a Glance 2019: Russian Federation. Available at: https://www.oecd.org/education/education-at-a-glance/EAG2019_CN_RUS.pdf (accessed 22 May 2022).

O'Kane P, Sezer S and Carlin D (2018) Evolution of ransomware. *IET Networks* 7(5): pp. 321-327.

Olayemi O (2014) A socio-technological analysis of cybercrime and cyber security in Nigeria. *International Journal of Sociology and Anthropology*, 6(3): pp. 116-125.

Ortner D (2015) Cybercrime and Punishment: The Russian Mafia and Russian Responsibility to Exercise Due Diligence to Prevent Trans-boundary Cybercrime. *Brigham Young University Law Review* 2015(1): pp. 177-218.

Pace D and Style J (1975) *Organized crime: concepts and control*. Englewood Cliffs: Prentice-Hall.

Paganini P (2022) Organizations paid at least $602 million to ransomware gangs in 2021. Available at: https://securityaffairs.co/wordpress/127974/cyber-crime/ransomware-payments-600m-2021.html (accessed 18 September 2022).

Palvia P, Ghosh J, Jacks T and Serenko A (2021) Information technology issues and challenges of the globe: the world IT project. *Information & Management* 58(8): pp. 1-15

Paoli L (2015) Mafia, Camorra, and 'Ndrangheta. In: Jones E and Pasquino G (eds) *The Oxford Handbook of Italian Politics*. Oxford: Oxford University Press, pp. 668-682.

Park J, Cho A, Lee J and Lee B (2019) The Economics of Cybercrime: The Role of Broadband and Socioeconomic Status. *ACM Transactions on Management Information Systems* 10(4): pp. 1-23

Park J (2021) The Lazarus Group: The Cybercrime Syndicate Financing the North Korea State. *Harvard International Review* 42(2): pp. 34-39.

Patten M and Newhart M (2018) *Understanding Research Methods. An Overview of Essentials.* New York: Routledge.

Potter R (2016) Cyberattacks and the Authoritarian Context. Available at: https://thediplomat.com/2016/10/cyberattacks-and-the-authoritarian-context/ (accessed 24 June 2022).

Radio Free Europe (2022) Jailed Former Sakhalin Governor Sentenced To 15 Years in Second Corruption Case. Available at: https://www.rferl.org/a/russia-sakhalin-governor-khoroshavin-jail-corruption/31825330.html (accessed 1 July 2022).

Rankin J (2014) Russian oligarch's arrest a warning from Putin, says hedge fund boss. The Guardian. Available at: https://www.theguardian.com/business/2014/sep/21/oligarch-arrest-warning-from-putin-says-bill-browder (accessed 5 July 2022).

Reeder J and Hall T (2021) Cybersecurity's Pearl Harbor Moment: Lessons Learned from the Colonial Pipeline Ransomware Attack. *The Cyber Defense Review* 6(3): pp. 15-40.

Remington T (2018) Russian Economic Inequality in Comparative Perspective. *Comparative Politics* 50(3): pp. 395-416.

Reuter P and Paoli L (2020) How Similar Are Modern Criminal Syndicates to Traditional Mafias? *Crime and Justice* 49(1): 223-287.

Richardson R and North M (2017) Ransomware: Evolution, Mitigation & Prevention. *International Management Review* 13(1): pp. 10-21.

Romo V (2021) Panic Drives Gas Shortages After Colonial Pipeline Ransomware Attack. NPR. Available at: https://www.npr.org/2021/05/11/996044288/panic-drives-gas-shortages-after-colonial-pipeline-ransomware-attack (accessed 29 April 2021).

Roth A (2022) Putin's security men: the elite group who 'fuel his anxieties'. The Guardian. Available at: https://www.theguardian.com/world/2022/feb/04/putin-security-elite-siloviki-russia (accessed 1 October 2022).

Russell M (2018) Socioeconomic inequality in Russia. Report for European Parliamentary Research Service. Report no. 620.225, April. France.

Ryan M (2021) *Ransomware Revolution: The Rise of a Prodigious Cyber Threat.* Switzerland: Springer.

Saarinen J (2022) Russians arrest REvil ransomware raiders. ITNews. Available at: https://www.itnews.com.au/news/russians-arrest-revil-ransomware-raiders-574733 (accessed 29 June 2022).

Sachs J (1992) The Economic Transformation of Eastern Europe: The Case of Poland. *Economics of Planning* 25: pp. 5–19.

Saric I (2019) Russian Anti-corruption Official Jailed for Corruption. Available at: https://www.occrp.org/en/daily/9925-russian-anti-corruption-official-jailed-for-corruption (accessed 2 September 2022).

Schneider E (2008) The Russian Federal Security Service under President Putin. In: White S (ed.) *Politics and the Ruling Group in Putin's Russia.* New York: Palgrave Macmillan, pp. 42-62.

Schulze G, Sjahrir B and Zakharov N (2016) Corruption in Russia. *The Journal of Law and Economics*, 59(1): pp. 135-171.

Schwartz C (1979) Corruption and Political Development in the U.S.S.R. *Comparative Politics* 11(4): pp. 425-443.

Shapiro D (2021) *The Gig Mafia: How Small Networks and High-Speed Digital Funds Have Changed the Face of Organized Crime*. New York: Business Expert Press.

Sharma A (2021) DarkSide reportedly received over $90m in Bitcoin from 47 victims before shutting down. Available at: https://www.thenationalnews.com/business/technology/darkside-reportedly-received-

over-90m-in-bitcoin-from-47-victims-before-shutting-down-1.1225655 (accessed 27 September 2022).

Shearer D (1998) Crime and Disorder in Stalin's Russia. A Reassessment of the Great Retreat and Origins of Mass Repression. *Cahiers du Monde russe* 39(1/2): pp. 119-148.

Shelley L (1995) Organized Crime in the Former Soviet Union. *Problems of Post-Communism* 42(1): pp. 56-60.

Shelley L (2003) Russia and Ukraine: Transition or Tragedy? In: Godson R (ed) *Menace to Society*. *Political-Criminal Collaboration Around the World*. USA: Transaction Publishers, pp. 199-230.

Shevchenko A (2007) The evolution of self-defense technologies in malware. Available at: https://securelist.com/the-evolution-of-self-defense-technologies-in-malware/36156/ (accessed 27 September 2022).

Shinar C (2016) Organized Crime in Russia. *European Review* 24(4): pp. 631-640.
Shkolnikov A (2008) From State Capture to State Capitalism: A Political Economy of Russia's Transition (1991-2007). PhD Thesis, George Mason University, USA.

Shlapentokh V (1993) *The Last Years of the Soviet Empire: Snapshots from 1985-1991*. Connecticut: Praeger Publishers.

Sibley N (2022) West Has Let Russian Oligarchs Hide Their Wealth Here For Far Too Long. Available at: https://www.hudson.org/research/17578-west-has-let-russian-oligarchs-hide-their-wealth-here-for-far-too-long (accessed 3 October 2022).

Siegel D (2012) Vory v zakone: Russian Organized Crime. In: Siegel D and van de Bunt H (eds) *Traditional Organized Crime in the Modern World.* New York: Springer Science+Business Media, pp. 27-47.

Sjouwerman S (2022) Conti Ransomware Attacks Reap in $180 Million in 2021 as Average Ransomware Payments Rise by 34%. Available at: https://blog.knowbe4.com/conti-ransomware-attacks-reap-in-180-million-in-2021-as-average-ransomware-payments-rise-by-34 (accessed 30 September 2022).

Smith S, Clark W, Viforj R, Wood G, Lisowski W and Truong K (2022) Housing and economic inequality in the long run: The retreat of owner occupation, *Economy and Society*, 51(2): pp. 161-186

Snowden N (2021) Triple Extortion Ransomware: A New Challenge for Defenders. Available at: https://blog.morphisec.com/triple-extortion-ransomware-a-new-challenge-for-defenders (accessed 30 April 2022)

Soldatov A and Borogan I (2015) *The Red Web: The Kremlin's Wars on the Internet*. New York: PublicAffairs.

Statista (2022) Median salary in job offers in the information technology (IT) sector in Russia from 2019 to 2021. Available at: https://www.statista.com/statistics/1307990/russia-offered-it-salary/ (accessed 5 June 2022).

Steadman I (2012) The Russian underground economy has democratized cybercrime, Available at: https://arstechnica.com/tech-policy/2012/11/the-russian-underground-economy-has-democratized-cybercrime/?comments=1&post=23460808 (accessed 25 August 2022).

Stone J (2020) Rare cybercrime enforcement in Russia yields 25 arrests, shutters 'BuyBest' marketplace. Available at: https://www.cyberscoop.com/buybest-hackers-arrested-fsb-russia/ (accessed 4 September 2022).

Suslov M (2020) Russian Conservatism as an Ideology: The Logic of Isolationism. In: Suslov M and Uzlaner D (eds.) *Contemporary Russian Conservatism. Problems, Paradoxes, and Perspectives.* Leiden: Brill, pp. 77-102.

Suslov M and Uzlaner D (2020) Dilemmas and Paradoxes of Contemporary Russian Conservatism: Introduction. In: Suslov M and Uzlaner D (eds.) *Contemporary Russian Conservatism. Problems, Paradoxes, and Perspectives.* Leiden: Brill, pp. 3-35.

Svendsen A (2018) Intelligence, Surveillance and Reconnaissance. In: Galbreath D and Deni J (eds) *Routledge Handbook of Defence Studies*. London: Routledge, pp. 272-287.

Symantec (2019) 2019 Internet Security Threat Report. Report for Symantec, February, Mount View, USA.

Tade O (2016) Meet the 'Yahoo boys' – Nigeria's undergraduate conmen. The Conversation. Available at: https://theconversation.com/meet-the-yahoo-boys-nigerias-undergraduate-conmen-60757 (accessed 24 May 2022).

Tamkin E (2017) Estonia: 10 years after its cyber attacks. Australian Financial Review. Available at: https://www.afr.com/companies/estonia-10-years-after-its-cyber-attacks-20170501-gvwbdh (accessed 30 June 2022).

TeamPassword (2021) Who is Fancy Bear and how can you protect yourself. Available at: https://teampassword.com/blog/who-is-fancy-bear-and-how-can-you-protect-yourself (accessed 29 March 2022).

The Associated Press (2021) How the Kremlin provides a safe harbor for ransomware. NBC News. Available at: https://www.nbcnews.com/tech/security/kremlin-provides-safe-harbor-ransomware-rcna699 (accessed 24 June 2022).

The Economist (2017) Russian oligarch Vladimir Yevtushenkov falls from grace, again. Available at: https://www.economist.com/business/2017/07/06/russian-oligarch-vladimir-yevtushenkov-falls-from-grace-again (accessed 1 October 2022).

The Moscow Times (2019) Half of Working Russians Earn Less Than $550 a Month. Available at: https://www.themoscowtimes.com/2019/07/19/welcome-to-the-russian-dacha-a66493 (accessed 3 October 2022).

The United States Department of Justice (2014) U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator. Available at: https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware (accessed 12 August 2022).

The United States Department of Justice (2018) North Korean regime-baked programmer charged with conspiracy to conduct multiple cyber attacks and intrusions. Available at: https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and (accessed 29 April 2022).

The World Bank (2021) School enrolment, tertiary (% gross) – Nigeria. Available at: https://data.worldbank.org/indicator/SE.TER.ENRR?locations=NG (accessed 24 May 2022).

Tidy J (2022) 74% of ransomware revenue goes to Russia-linked hackers. BBC. Available at: https://www.bbc.com/news/technology-60378009 (accessed 3 May 2022).

Tomass M (1998) Mafianomics: How Did Mob Entrepreneurs Infiltrate and Dominate the Russian Economy? *Journal of Economic Issues* 32(2): pp. 565-574.

Trading Economics (2022) Russia Unemployment Rate. Available at: https://tradingeconomics.com/russia/unemployment-rate (accessed 4 June 2022).

Transparency International (2022) Corruption Perception Index 2021. Report, Transparency International, Germany, January.

Trend Micro Research (2021a) An Overview of the DoppelPaymer Ransomware. Available at: https://www.trendmicro.com/en_us/research/21/a/an-overview-of-the-doppelpaymer-ransomware.html (accessed 30 June 2022).

Trend Micro Research (2021b) What We Know About the DarkSide Ransomware and the US Pipeline Attack. Available at: https://www.trendmicro.com/en_ca/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html (accessed 18 September 2022).

Tropina T (2013) Organised Crime in Cyberspace. In: Stiftung H and Schönenberg R (eds) *Transnational Organized Crime: Analyses of a Global Challenge to Democracy*. Bielefeld: Transcript Verlag, pp. 47-60.

Turner A, McCombie S and Uhlmann A (2019) A target-centric approach to WannaCry 2.0. *Journal of Money Laundering Control* 22(4): pp. 646-665.

Uchill J (2022) Russia makes more arrests, but cybercrime-harboring reputation hard to shake. Available at: https://www.scmagazine.com/analysis/policy/russia-makes-more-arrests-but-cybercrime-harboring-reputation-hard-to-shake (accessed 31 March 2022).

Unit 42 (2021) Threat Assessment: DoppelPaymer Ransomware. Available at: https://unit42.paloaltonetworks.com/ransomware-threat-assessments/4/ (accessed 30 April 2022).

United States Department of the Treasury (2019) Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware. Available at: https://home.treasury.gov/news/press-releases/sm845 (accessed July 2022).

Vaas L (2021) Ransomware Payments Explode Amid 'Quadruple Extortion'. Available at: https://threatpost.com/ransomware-payments-quadruple-extortion/168622/ (accessed 30 April 2022).

Vaisburd V, Simonova M, Bogatyreva I, Vanina E and Zheleznikova E (2016) Productivity of Labour and Salaries in Russia: Problems and Solutions. *International Journal of Economics and Financial Issues* 6(S5): pp. 157-165.

Vaksberg A (1991) *The Soviet Mafia*. Translated by J Roberts and E Roberts. London: Weidenfeld and Nicolson.

Varese F (1998) The society of the vory-v-zakone, 1930s-1950s. *Cahiers du monde russe : Russie, Empire russe, Union soviétique, États indépendants* 39(4): pp. 515-538.

Varese F (2001) *The Russian Mafia: Private Protection in a New Market Economy*. Oxford: Oxford University Press.

Vavra S (2021) The Mafia Finds a New Frontier for Crime: the Internet. Available at: https://www.thedailybeast.com/the-mafia-finds-a-new-frontier-for-crime-the-internet (accessed 30 September 2022).

Vershinin M (2004) Modern youth subcultures. Available at: https://psyfactor.org/lib/vershinin4.htm (accessed 3 October 2022).

Verizon (2022) Data Breach Investigations Report. Report, Verizon, USA, May.

Vincent M (2020) *Criminal Subculture in the Gulag. Prisoner Society in the Stalinist Labour Camps, 1924-53.* London: Bloomsbury Academic.

Wall D (2021) The Transnational Cybercrime Extortion Landscape and the Pandemic: changes in ransomware offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin* 22: pp. 1-16.

Walker S (2017) Unequal Russia: is anger stirring in the global capital of inequality? The Guardian. Available at:

https://www.theguardian.com/inequality/2017/apr/25/unequal-russia-is-anger-stirring-in-the-global-capital-of-inequality (accessed 9 June 2022).

Wang Q and Li M (2012) Home computer ownership and Internet use in China: Trends, disparities, socioeconomic impacts, and policy implications. *First Monday* 17(2).

Ward M (2014) Cryptolocker victims to get files back for free. BBC. Available at: https://www.bbc.com/news/technology-28661463 (accessed 19 April 2022).

Ward T (2022) Military history is repeating for Russia under Putin's regime of thieves. Available at: https://theconversation.com/military-history-is-repeating-for-russia-under-putins-regime-of-thieves-181164 (accessed 24 June 2022).

Warren P (2007) Hunt for Russia's web criminals. The Guardian. Available at: https://www.theguardian.com/technology/2007/nov/15/news.crime (accessed 30 September 2022)

Weber V (2022) Financial Incentives May Explain the Perceived Lack of Ransomware in Russia's Latest Assault on Ukraine. Available at: https://www.cfr.org/blog/financial-incentives-may-explain-perceived-lack-ransomware-russias-latest-assault-ukraine (accessed 27 September 2022).

Westman N (2020) Woman dies during a ransomware attack on a German hospital. The Verge. Available at: https://www.theverge.com/2020/9/17/21443851/death-ransomware-attack-hospital-germany-cybersecurity (accessed 27 September 2022).

Wheatley J (2021) Transnational Organized Crime. A Survey of Laws, Policies and International Conventions. In: Allum F and Gilmour S (eds) *The Routledge Handbook of Transnational Organised Crime*. London: Routledge, pp. 51-66.

Wolske J (2000) Jack, Judy, Sam, Bobby, Johnny, Frank...: An investigation into the alternate history of the CIA-Mafia collaboration to assassinate Fidel Castro, 1960–1997. *Intelligence and National Security* 15(4): pp. 104-130.

Wood M (2021) Rethinking How Technologies Harm. *British Journal of Criminology* 16(3): pp. 627-647.

Williams A (2022) A Look Back at The USSR Computer Industry. Available at: https://hackaday.com/2022/07/16/a-look-back-at-the-ussr-computer-industry/ (accessed 25 September 2022).

Xiao J (2016) The Evolution of Russian Organised Crime and the Challenge to Democracy. Available at: https://www.e-ir.info/2016/07/31/the-evolution-of-russian-organised-crime-and-the-challenge-to-democracy/ (accessed 2 September 2022).

Yip M, Shadbolt N, Triopanis T and Webber C (2012) The Digital Underground Economy: A Social Network Approach to Understanding Cybercrime. In: *Digital Futures conference*, Aberdeen, 23-25 October 2012, pp: 1-3

Young A and Yung M (1996) Cryptovirology: Extortion-Based Security Threats and Countermeasures. In: *Proceedings 1996 IEEE Symposium on Security and Privacy*, Oakland, USA, 6-8 May 1996, pp. 129-140. IEEE.

Zabrisky Z (2020) Pure Poison: Putin's Links to Espionage, Terrorism and Organised Crime. Available at: https://bylinetimes.com/2020/08/27/pure-poison-putins-links-to-espionage-terrorism-and-organised-crime/ (accessed 20 July 2022).

Zaharia A (2022) Everything you need to know about CryptoWall. Available at: https://heimdalsecurity.com/blog/cryptowall-ransomware/ (accessed 19 April 2022).

Zhang J and Wang Y (1995) *The emerging market of China's computer industry*. Connecticut: Quorum Books.

Zhu X and Lin S (2019) *Equity Index Construction and Research on Wealth Gap*. Singapore: Springer Singapore.

Zetter K (2016) Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. Wired. Available at: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/ (accessed 18 September 2022).

Zorz (2017) NotPetya attacker can't provide decryption keys, researchers warn. Available at: https://www.helpnetsecurity.com/2017/06/29/notpetya-decrypt-fail/ (accessed 24 April 2022).