International Journal of Economics and Finance; Vol. 15, No. 5; 2023
ISSN 1916-971X E-ISSN 1916-9728
Published by Canadian Center of Science and Education

Financial Perspective Thought Experiment on Russian Cyber Threat Actors

Zsolt Bederrna[1]

[1] Doctoral School on Safety and Security Sciences, Obuda University, Bécsi út 96/b H-1034 Budapest, Hungary

Correspondence: Zsolt Bederna, Doctoral School on Safety and Security Sciences, Obuda University, Bécsi út 96/b H-1034 Budapest, Hungary. ORCID 0000-0003-0444-7275.

Received: February 1, 2023 Accepted: March 16, 2023 Online Published: March 30, 2023

doi:10.5539/ijef.v15n5p1 URL: https://doi.org/10.5539/ijef.v15n5p1

Abstract

Due to the advancement of information and communication technology and related services, the digital world has reached many people, private companies, and governments, and meanwhile, threat actors regarding motivation, knowledge, and capabilities have also evolved, and thus, today, they compete and collaborate with others. Financially motivated threat actors also do businesses; as such, with a higher sophistication level, they create tools and provide them as Malware as a Service (MaaS) for renting, and if they can extract accounts, they launder those amounts of cash through hardly traceable channels. In contrast, state-sponsored threat actors act according to the government's political and military needs.

The Russian government lets independent threat actors freely conduct various cyberattacks, including cyber espionage, sabotage, and ransomware attacks on non-Russian geolocations and entities, meanwhile financing its threat actors to achieve social and political activities. As such, providing a thought experiment, the paper examines the potential income of a for-profit organization, the related tax income, and the costs of operating a government-related threat actor. To conduct the analysis, it provides a methodological approach and applies that to TA542 and APT28 threat actors, using inputs from open-source intelligence.

Keywords: cyber threat, financial analysis, Russia, TA542, APT28

1. Introduction

Technology, as one of the most decisive factors of the information society, provides information and communication technology (ICT) services manifesting cyberspace, infiltrating the everyday activities of people, companies, and government entities. As a result of the dynamic ICT development, society has a dominant and growing dependence on that (Sun et al., 2021). According to Kuehl (Kuehl, 2009, p. 28), cyberspace is "a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange and exploit information via interdependent and interconnected networks using information-communication technologies". In cyberspace, however, several actors operate unintendedly and intendedly maliciously, having their objectives, preferences, tools, and tactics (Emmanuel, 2017, p. 45). The actors behave according to their visions and objectives that determine the strategies and payoffs for actions. These actors can be considered players who play a big game in cyberspace, limited by resource constraints. On one side, there are threat actors or agents as attackers conducting malicious actions; on the other, there are the defenders that act legally.

Defenders are required for a constantly increasing effort to tackle cybersecurity because threat actors and cybercrimes have evolved, providing a changing environment. For example, concentrating on threat actors' activities affecting the European Union, the European Union Agency for Cybersecurity (ENISA) publishes its strategic-level cyber threat intelligence called Threat landscape, such as (ENISA, 2022; Theocharidou et al., 2021) in which the growing trends unfolded.

The Russian government passively and actively engages in malicious activities in cyberspace (Kari & Pynnöniemi, 2019). This approach lets independent and state-sponsored threat actors freely conduct various cyberattacks, including cyber espionage, sabotage, and ransomware attacks on non-Russian geolocations and entities, including citizens, for-profit companies, public organizations, and governments, and conduct social and political activities. This strategic approach raises the following questions. (1) What is the probable income of a for-profit organization? 2) What are the costs of operating a government-related threat actor?

To conduct the analysis, the paper provides literature review of cyberthreat actors' characterization in Section 2 and methodological approach in Section 3 that we follow later the chosen TA542 and APT28 threat actors in Section 4. Lastly, Section 5 summarizes and concludes the study. Although we aim to use as precise input as possible via open-source intelligence (OSINT), such information is hardly available and incomplete.

2. Literature Review of Cyberthreats' Characterization

The Structured Threat Information Expression (STIX) (OASIS, 2021), which is a prominent standard describing just-in-time information of cyber threats, gives a vocabulary to define threat sophistication levels (called *threat-actor-sophistication-ov*) as *none*, *minimal*, *intermediate*, *advanced*, *expert*, *innovator*, and *strategic*. The different levels reveal that the various capabilities induce differences in the fulfilled functions. Some threat actors can only use the tools created by others, while sophisticated actors make and maintain them. Therefore, it is not surprising that these malicious actors not only compete with each other but also cooperate, since, like botnets, the development of comprehensive and sophisticated tools requires the involvement of several actors. According to Miller (2010), several competencies are involved in development and operation, such as vulnerability analysts, exploit developers, bot collectors, bot maintainers, operators, remote personnel, developers, testers, sysadmins, and managers, which must cost high.

Furthermore, the different sets of competencies and capabilities provide the demand and supply for the Cybercrime as a Service business model (Manky, 2013) as (1) the Crimeware as a Service, (2) the Cybercrime Infrastructure as a Service, and (3) the Hacking as a Service. Crimeware as a Service comprises general or specifically targeted identified vulnerabilities and related exploits, such as zero-day vulnerabilities and malware (Szőr, 2005). Today, the Cybercrime Infrastructure as a Service is also called as Malware as a Service (MaaS), providing "threat actors with a remunerated botnet service that allows them to disseminate malware" (Tudor, 2022). Cybercrime Infrastructure as a Service comprises infrastructural elements, specifically clients and servers, allowing others to rent an entire botnet or typically a part of a botnet with a limited set of capabilities, such as spamming and spyware (Bederna & Szádeczky, 2019). If a botnet is used to extract cash from victims' accounts, threat actors launder those amounts of cash with complicated, hardly traceable methods (Custers et al., 2019). Hacking as a Service encompasses the ability of a cyberattack to be completely outsourced to a "service provider", including planning and performing on-demand.

At the same time, the objectives for which self-made or rented tools are chosen are mainly affected by capabilities and personal and organizational motives. Personal motivation integrates the source of motives such as biological, social, and psychological needs, wants, or desires and the probable effects of any given action (Deci & L., 2000), shaping the organization-level intentions, for which the STIX's *attack-motivation-ov* vocabulary (OASIS, 2021) provides a list of possible motivations. This vocabulary structures the intensity and the persistence of an attack and allows defenders to better understand likely targets and threat behaviors. It comprises *accidental*, *coercion*, *dominance*, *ideology*, *notoriety*, *organizational-gain*, *personal-gain*, *personal-satisfaction*, *revenge*, and *unpredictable* values using the Threat Agent Motivations created by Casey (2007). In this context, personal and organizational levels are characterized by financial and non-financial objectives, from which the second type of threat actors are typically operated by governments. We are working with the organizational threat actors in the paper to analyze their financial behavior. However, studying cyber threat actors in such a nonconventional way lacks research.

3. Methodology Development

3.1 The General Concept

Analyzing a bunch of cash flow (CF) arising at a different time in the examined interval needs a specific approach given by discounted cash-flow methodologies. These methodologies involve forecasting future cash flows and then discounting them to their present value at a rate that reflects their riskiness. So, the valuation of a project or a whole company based on projected future cash flows is adjusted for the time value of money to calculate the present value (PV) to determine the net present value (NPV). A project evaluation works with cash flows within the forecast period and the terminal value that represents the cash flow stream after the forecast period (Fernández, 2007), for which we choose the perpetual growth to the terminal value. The perpetual growth (Gordon Growth Model) (Gordon & Shapiro, 1956) assumes that the given activity will continue to generate cash flows at a constant rate. The exit multiple expects that the company will be sold for a multiple of some market metric.

To determine the value of the expected expenses and returns before starting the investment, one must apply the following formula:

$$NPV = \overbrace{\sum_{t=1}^{n} \frac{CF_t}{\prod_{i=1}^{t}(1+r_i)}}^{explicit\ interval} + \frac{\overbrace{\frac{CF_n*(1+g)}{r_{n+1}-g}}^{terminal\ value}}{\prod_{i=1}^{n}(1+r_i)} \quad (1)$$

where

CF_t is the annual cash flow,

r_i is the yearly interest rate,

g is the expected growth rate.

3.2 Discount Rates

Although NPV calculation is an essential tool in investment calculation, it has drawbacks (Gaspars-Wieloch, 2019), one of which is the sensitivity to determining reasonable interest rates. Furthermore, evaluating a private company or a government project requires different treatment.

3.2.1 Discount Rate of a Private-Company Threat Actor

From a financial perspective, most assets are exposed to risk, and riskier investments need higher compensation returns. A prominent solution is the Capital Asset Pricing Model (CAPM) (Sharpe, 1964) for calculating the cost of capital, discussed in detail in (Elbannan, 2014), giving the following formula:

$$r_E = r_f + \overbrace{\beta\left(r_M - r_{f,nom}\right)}^{risk\ premium} \quad (2)$$

where

r_E represents the shareholder's interest rate,

r_f is the risk-free interest rate,

r_M is the market interest rate,

$r_{f,nom}$ is the nominal risk-free interest rate, and

β (beta) is the measure of the volatility of an individual stock compared to the systematic risk of the entire market.

In the above equation, the $\beta\left(r_M - r_{f,nom}\right)$ together is the risk premium that an investor expects to receive from holding a particular stock or portfolio above the risk-free assets.

In that case, the given entity does not use any debt (D) for its operation ($D = 0$), i.e., it is considered as unleveraged, and so, no tax shield would decrease the payable taxes. In this case, the corporate interest rate equals the shareholder interest rate. On the other hand, if a company is leveraged, the weighted-average cost of capital (WACC) must be considered, discussed in detail by Frank et al. (2016). The WACC encompassing the tax shield is calculated by the following formula:

$$r_{wacc} = \frac{E}{E+D} * E(r_E) + (1 - t_c) * \frac{D}{E+D} * E(r_D) \quad (3)$$

where

r_{wacc} represents the WACC,

$E(\cdot)$ represents the expected value,

E is the shareholder value (as before),

D is the creditor value,

r_E represents the shareholder's interest rate (as before),

r_D is the creditor's interest rate, and

t_c is the corporate tax rate.

Unless the threat actor has a legally registered entity, it is not entitled to borrow from legal entities, but at the same time, it is not required to pay taxes. However, because we are examining the specific scenario when a threat actor how much tax would pay if it were a legal entity, we consider the TA542 threat actor as an unleveraged company. At the same time, except the threat-actor private company is not only a legal entity but a publicly traded firm (which is obviously not), it operates the business with higher risks, represented by the total beta defined by Damodaran (2012). The total beta is calculated with the following formula:

$$\beta_T = \beta_M * p_{jM} \quad (4)$$

where

β_T is the total beta,

β_M is the market beta,

p_{jM} is the correlation between the stock and the index.

The total beta has a higher value than the market beta, depending upon the correlation between the firm and the market, since a threat actor may tackle fluctuating income and higher personal risks of being a sitting duck and, in the case of a wrong step, its members being arrested.

3.2.2 Discount Rate of a Government Threat Actor

Calculating the cost of capital for public projects needs special attention because of the limited quantifiability of the benefits. Two estimates are generally available for public projects, which are the social rate of time preference (SRTP) and the social opportunity cost of capital (SOC) (Kazlauskienė, 2015). The commonly accepted method of calculating SRTP is the Ramsey formula (Ramsey, 1928):

$$S = p + eg \quad (5)$$

where:

S is the social discount rate,

p is the utility discount rate,

e is the elasticity of the marginal utility of consumption,

g the expected rate of growth per capita.

The SOC approach is based on the race of private and public projects for funds. So that the returns of public projects cannot fall below the returns of the competing private projects; else, the community welfare would require the reallocation of funds (Kazlauskienė, 2015). There are more estimations of the SOC value, such as the high-grade corporate bonds (Moore et al., 2004) and the marginal pretax rate of return on riskless private investments (Zhuang et al., 2007).

3.3 Identifying Typical Cash Flows of Threat Actors

The other factor to which NPV calculation is sensitive is the properly determined cash flows, i.e., having data on projected income and cost statements (Gaspars-Wieloch, 2019). This fact is especially true for the public-project appraisal because of the intangible nature of public services or, in the case of charging for services, insufficient cash flows (Brzozowska, 2007).

A threat actor posing to function as a private organization is interested in profit generation. Its income originates from successful cyberattacks by paid ransoms or sold data it steals (by applying spyware). Furthermore, if the given actor is highly sophisticated, then it can develop cyberattack tools to be sold or rented. On the other hand, a government-sponsored threat actor working for non-financial objectives like data theft and sabotage should have only a fixed funding income.

Regarding operational expenditure (OPEX), one of the most significant components must be labor costs. The credit-related costs, including, e.g., the interest on the debt (if any), are in OPEX as well as the infrastructure for the internal operation and for attacking if they are rented; otherwise, they fit in the capital expenditure (CAPEX). In the last case, amortization's effect must be considered, too. However, since, threat actors generally use computers as part of the botnets (Bederna & Szádeczky, 2019) to conduct cyberattacks for which devices are held, operated, and maintained by others.

3.4 Evaluation Methods

Since we are examining the two cases from different perspectives, we select two different methodologies. APT28's case, being a state-sponsored threat actor, encompasses cost-related cash flows for which we use NPV calculation with an available social discount rate series regarding Russia.

On the other hand, TA552's case needs a more comprehensive evaluation methodology, due to the financial motives they operate, to determine or at least infer its profitability regarding, examine financial-related decision points, and the tax that it would pay for the government if it were a legal entity. However, such evaluation methodologies differ in the details of their execution, such as how they account for the value created or destroyed and, therefore, in the input types with which they work (Fernández, 2007). Despite the wide application of Discounted Cash Flows (DCF) (Fisher, 1930), it demands far more input than we can produce or

infer more or less. So we use the Adjusted Present Value (APV) (Myers, 1974). APV's approach is to analyze financial maneuvers separately, then add their value to that of the business, it involves less input in the calculation of company assets, and it uses r_E to discount cash flows assuming unleveraged operations.

4. Hypothetical Case Studies

4.1 Supplementary Data

In the analysis of TA542 and APT28 data, we use the supplementary data displayed in Table 1. Furthermore, we take amortization linearly in five years, commencing next month from the purchase date (Fenebris, 2020), but assuming the purchases happen at the very beginning of each year, and we take the amount of the minimum wages with a multiplicity factor being 20.

Table 1. Supplementary data for case studies

	2014	2015	2016	2017	2018	2019	2020
Yearly averaged RUB to USD (ExchangeRates, 2023)	0.0265	0.0165	0.015	0.0172	0.016	0.0155	0.0139
Minimum monthly Russian wages in RUB (WageIndicator Foundation, 2023)	5 554	5 965	6 204	7 650*	10 326**	11 280	12 130
Russian inflation rate (Macrotrends, 2023)	7.82%	15.53%	7.04%	3.68%	2.88%	4.47%	3.38%
Corporate tax rate in Russia (Expatica, 2022)	20%	20%	20%	20%	20%	20%	20%
SRTP in Russia (Kossova & Sheluntcova, 2016)	3.2%	3.2%	3.2%	3.2%	3.2%	3.2%	3.2%
Unleveraged total beta for Russian Software (Internet) companies (Damodaran, 2022)	12.92%	14.99%	17.03%	17.82%	13.59%	14.36%	11.88%

Note. *Calculated as the average of the two available data for the year.

**Calculated as the average of the data available for January and December.

Source: the author.

4.2 TA542 – A Private-Company Project

4.2.1 Short Introduction of TA542

Based on the threat intelligence report of the CERT-FR (2021), which is the French governmental Computer emergency response team (CSIRT), the TA542 threat actor is seemingly a Russian cybercriminal group responsible for Emotet botnet that was initially recognized in 2014 as a banking trojan. Its first three versions targeted banking clients to carry out automatic fraudulent transfers from compromised bank accounts. However, until 2015, others could initiate such transfers because TA542 sold Emotet on underground forums at that time. After that, Emotet became available to a possibly limited set of clients. In 2017, TA542 removed Emotet's banking-trojan-horse capability and modified the botnet to be able to distribute other malware, becoming a MaaS that are self-operated modules (such as spamming, credential stealing, email harvesting, and spreading on local networks (Proofpoint, 2019)) or operated by TA542's clients, separating three independent infrastructures, named Epoch 1, Epoch 2, and Epoch 3. These botnets were inactive several times a year for maintenance and hiding.

Although law enforcement and judicial authorities worldwide disrupted Emotet in January 2021 (EUROPOL, 2021), it resumed operations in November 2021, running on two separate infrastructures, identified as Epoch 4 and Epoch 5 (Duncan, 2022). The fact of the return is not surprising, as TA542 is continually improving the applied tactics, techniques, and procedures (Paganini, 2022).

4.2.2 Data and Analysis

Although the TA542 group's botnet has been active since 2014, there was a decision point in 2017 on whether it should remain as a banking trojan or be modified to be a MaaS, respectively denoted as Alternative A and Alternative B. We check the alternatives based on available data and rough estimates.

For Alternative A, displayed in Table 2, we consider that the banking trojan was rented for \$600 (Deloitte, 2018, p. 15) in 2017, increasing annually with the inflation rate, with 100 times usage per month from 2014. At the same time, the group uses Emotet to infect victims' machines, and account transfers 1 000 times yearly with \$700 (Custers et al., 2019, p. 13) on average without inflation. Believing a smaller organization, the labor count is 10. The CAPEX encompasses \$500 thousand in investments annually, growing by the inflation rate.

On the other hand, in the case of Alternative B, depicted in Table 3, the income origins from MaaS renting services and profit shares on incomes of Emotet's customers (CERT-FR, 2021, p. 7). Using this information, we take that the MaaS renting is \$2 000 with an amount of 500 for each "customer" and the MaaS profit share has

the amount of $2 million annually beginning with 2018. As far as publicly known, TA542 collaborated with several known and believed threat actors (CERT-FR, 2021, pp. 7-9), as Wizard Spider (Trickbot 2017-2020, Ryuk 2019-2020, Conti, 2020), Lunar Spider (IceId 2017-2018, AZORult 2018-2020), Doppel Spider (DoppelDridex 2019-2020), Evil Corp (Dridex 2017-2020, Dridex 2017-2020), and Black Basta (QakBot 2017-2020). Moreover, there are botnets with unknown threat actors with which T542 worked, like ZeusPanda (2018), UmbreCrypt (2017), SilentNight (2020), and Noselesn (2018-2019).

The nearest approximation regarding the extent of a threat actor's membership that has been publicly found is Trickbot. In 2022, a current estimate said Trickbot had members between 100 and 400 (Burgess, 2022), from which we take a constant 100. Finally, we consider that CAPEX was initially $1 million, growing annually with the inflation rate, and use the unleveraged total beta for a Software (Internet) company as the cost of capital.

Although the two alternatives' evaluation takes thought-based inputs, the ratio between them must mirror the reality except for tax paying, unless TA542 would not have chosen to turn toward MaaS.

Table 2. TA542-related cost estimation thought experiment in the year 2017 on whether Emotet should remain as a banking trojan

	2017	2018	2019	2020
Revenue	**$1 420.00**	**$1 440.74**	**$1 473.85**	**$1 500.00**
Banking trojan	$720.00	$740.74	$773.85	$800.00
Account transfers	$700.00	$700.00	$700.00	$700.00
OPEX	**($415.79)**	**($499.40)**	**($527.09)**	**($515.77)**
Labor costs	($315.79)	($396.52)	($419.62)	($404.66)
Other costs	($100.00)	($102.88)	($107.48)	($111.11)
EBITDA	**$1 004.21**	**$941.34**	**$946.75**	**$984.23**
Depreciation	($0.00)	($0.00)	($0.00)	($0.00)
Amortization	($100.00)	($202.88)	($310.36)	($321.47)
EBIT	**$904.21**	**$738.46**	**$636.39**	**$662.76**
Taxes	($180.84)	($147.69)	($127.28)	($132.55)
Net income	**$723.37**	**$590.77**	**$509.11**	**$530.21**
CAPEX	**($500.00)**	**($514.40)**	**($537.39)**	**($555.56)**
PV	$274.46	$208.65	$184.31	$172.94
$NPV_{explicit}$	**$840.36**			
$PV_{implicit}$	$2 142.10			
$NPV_{explicit+implicit}$	**$2 982.45**			

Note. Amounts display values in thousands.

Source: the author.

Table 3. TA542-related cost estimation thought experiment in the year 2017 on whether Emotet should be modified to be a MaaS

	2017	2018	2019	2020
Revenue	**$5 000.00**	**$16 403.20**	**$12 747.87**	**$13 111.15**
MaaS renting	$5 000.00	$9 201.60	$7 373.94	$7 555.58
MaaS profit share	$5 000.00	$7 201.60	$5 373.94	$5 555.58
OPEX	**($3 257.92)**	**($4 068.06)**	**($4 303.64)**	**($4 157.68)**
Labor costs	($3 157.92)	($3 965.18)	($4 196.16)	($4 046.57)
Other costs	($100.00)	($102.88)	($107.48)	($111.11)
EBITDA	**$1 742.08**	**$12 335.14**	**$8 444.23**	**$8 953.47**
Depreciation	($0.00)	($0.00)	($0.00)	($0.00)
Amortization	($200.00)	($405.76)	($620.72)	($642.94)
EBIT	**$1 542.08**	**$11 929.38**	**$7 823.52**	**$8 310.53**
Taxes	($308.42)	($2 385.88)	($1 564.70)	($1 662.11)
Net income	**$1 233.66**	**$9 543.50**	**$6 258.81**	**$6 648.43**
CAPEX	**($1 000.00)**	**($1 028.80)**	**($1 074.79)**	**($1 111.12)**
PV	$368.07	$6 665.43	$3 792.71	$3 609.28
$NPV_{explicit}$	**$14 435.49**			
$PV_{implicit}$	$56 888.76			
$NPV_{explicit+implicit}$	**$71 324.25**			

Note. Amounts display values in thousands.

Source: the author.

4.3 APT28 – A Government Project

4.3.1 Short Introduction of APT28

Based on the review available in (Bederna & Szádeczky, 2019), APT28 is believed to be active since 2004; however, their activities have been revealed in more detail since 2014.

From late 2014 through 2016, the group covertly spied on the Ukrainian military by compromising an official mobile application developed by the Ukrainian military, affecting more than 9 000 artillery personnel. In 2016, it targeted the United States (US) Democratic political party, the Organization for Security and Cooperation in Europe (OSCE), Germany's Christian Democratic Union (CDU), and the World Anti-Doping Agency (WADA). At the beginning of 2017, group members attacked multiple International Olympic Winter Sports Federations due to the sanction affecting game participation. Later, they targeted the hospitality sector affecting individuals staying in hotels throughout Europe and the Middle East. Furthermore, APT28 compromised the German "Informationsverbund Berlin-Bonn" (IVBB) network, the German federal chancellery, the German parliament, federal ministries, the Federal Audit Office, and other security entities. In early February 2018, a new cyber espionage campaign of APT28 was recognized that targeted Ministries of Foreign Affairs.

4.3.2 Data and Analysis

To examine APT28-related costs, we take the years from 2014 to 2018 as the explicit interval when the group was already recognized and known to be frequently active. We consider a labor count of 500 based on (Miller, 2010), annual $1 million CAPEX growing by the inflation rate, and the SRTP as the cost of capital. As we evaluate only the cost-related cash flows, we use NPV. According to the rough estimate in Table 4, an APT28-like threat actor can be kept up with millions of dollars per year.

Table 4. APT28-related cost estimation

	2014	2015	2016	2017	2018
OPEX	**($17 661.72)**	**($11 810.70)**	**($11 167.20)**	**($15 789.60)**	**($19 825.92)**
Labor costs	($17 661.72)	($11 810.70)	($11 167.20)	($15 789.60)	($19 825.92)
CAPEX	**($1 000,00)**	**($1 155,30)**	**($1 236,63)**	**($1 282,14)**	**($1 319,07)**
PV	($18 083,06)	($12 174,37)	($11 285,40)	($15 050,78)	($18 063,79)
NPV	**($74 657,41)**				

Note. Amounts display values in thousands.

Source: the author.

5. Conclusion

The paper introduced methodologies to analyze financially motivated and state-sponsored threat actors, for which two Russian threat actors, the TA542 group and the APT28, were chosen. However, due to the minimal publicly available data determining cash flows and the hardness of selecting the proper cost of capital, their evaluations could be a thought experiment.

At the same time, applying the methodologies clearly shows that a financially motivated threat actor may work similarly from a financial perspective as the legal companies, as they must plan the operation and sometimes choose between projects they realize. However, as a remaining assumption, such threat actors take a higher beta value as legal companies operating in a comparable legal industry due to the increased risk of their activities. On the other hand, state-sponsored threat actors can pose to be a financial cost center meanwhile achieving hardly monetized political or military-like objectives. While the Russian cybercrime-related strategy regarding the financially motivated threat actors remains, the only points to avoid the proliferation of such activities is the proper planning, implementation, and maintenance of cybersecurity controls or the decreasing or prevention of their cash flows.

Based on the available data and achieved estimates, Russia relinquishes tax incomes for prejudicing non-Russian entities by financially motivated threat actors. In addition, it maintains with relatively low costs the state-sponsored threat actors; on the other hand, the expenditure for its operations is probably much higher than the unpaid tax by the financially motivated threat actors.

This behavior of Russia regarding cyberspace is unethical but successful, providing struggle and regular losses for entities in non-friendly territories and financial and non-financial gains for Russian entities. Strategies for pushing back the Russian adversarial cyber threat activities can be realized on the threat-actor level or state level.

At the threat-actor level, cybersecurity professionals are constantly involved in warding off cyberattacks. However, law enforcement can find threat actors less efficiently for arresting. They all need the help of politicians in the European Union, the United Kingdom, and the United States, e.g., in banning cybercriminals and properly acting on their sponsors.

Acknowledgments

The paper's appearance is financially supported by Cylair Consulting Ltd (Hungary).

The data presented in this study is openly available in Open Science Framework (OSF) at https://dx.doi.org/10.17605/OSF.IO/SHQ5G.

References

Bederna, Z., & Szádeczky, T. (2019). Cyber espionage through Botnets. *Security Journal*, *33*, 43-62. https://doi.org/10.1057/s41284-019-00194-6

Brzozowska, K. (2007). Cost-Benefit Analysis in Public Project Appraisal. *Engineering Economics*, *53*(3), 78-83. https://inzeko.ktu.lt/index.php/EE/article/view/12247

Burgess, M. (2022, January 2). *Inside Trickbot, Russia's Notorious Ransomware Gang*. Retrieved from https://www.wired.co.uk/article/trickbot-malware-group-internal-messages

Casey, T. (2007). Threat Agent Library Helps Identify Information Security Risks. In *Intel White Paper*. https://doi.org/10.13140/RG.2.2.30094.46406

CERT-FR. (2021). *The malware-as-a-service Emotet*. Retrieved from https://www.cert.ssi.gouv.fr/uploads/CERTFR-2021-CTI-003.pdf

Custers, B. H., Pool, R. L., & Cornelisse, R. (2019). Banking malware and the laundering of its profits. *European Journal of Criminology*, *16*(6), 728-745. https://doi.org/10.1177/1477370818788007

Damodaran, A. (2012). *Investment Valuation: Tools and Techniques for Determining the Value of Any Asset* (3rd ed.). John Wiley & Sons.

Damodaran, A. (2022). *Data:Archives, Discount Rate Estimation*. Retrieved from https://pages.stern.nyu.edu/~adamodar/New_Home_Page/dataarchived.html#discrate

Deci, R., & L., M. R. E. (2000). Self Determination Theory and the facilitation of intrinsic motivation, social development and well-being. *American Psychologist*, 68-78. https://doi.org/10.1037/0003-066X.55.1.68

Deloitte. (2018). *Black-market ecosystem Estimating the cost of "Pwnership"*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-risk-black-market-ecosystem.pdf

Duncan, B. (2022, May 17). *Emotet Summary: November 2021 Through January 2022*. Retrieved from https://unit42.paloaltonetworks.com/emotet-malware-summary-epoch-4-5/#Emotet-in-November-2021

Elbannan, M. A. (2014). The Capital Asset Pricing Model: An Overview of the Theory. *International Journal of Economics and Finance*, *7*(1), 216-228. https://doi.org/10.5539/ijef.v7n1p216

Emmanuel, C. A. (2017). Game Theory Basics and Its Application in Cyber Security. *Advances in Wireless Communications and Networks*. https://doi.org/10.11648/j.awcn.20170304.13

ENISA. (2022). *Threat Landscape 2022*. https://doi.org/10.2824/764318

EUROPOL. (2021). *World's most dangerous malware EMOTET disrupted through global action*. Retrieved from https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

ExchangeRates. (2023). *Russian Rouble (RUB) to US Dollar (USD) exchange rate history*. Retrieved from https://www.exchangerates.org.uk/RUB-USD-exchange-rate-history.html

Expatica. (2022, September 12). *Corporate tax in Russia*. Retrieved from https://www.expatica.com/ru/finance/taxes/corporate-tax-in-russia-1071356/

Fenebris. (2020). *What useful life should be considered when estimating the TAB factor of an intangible asset?* Retrieved from http://www.taxamortisation.com/tax-amortisation-benefit/russia.html

Fernández, P. (2007). Valuing companies by cash flow discounting: Ten methods and nine theories. *Managerial Finance*, *33*(11), 853-876. https://doi.org/10.1108/03074350710823827

Fisher, I. (1930). *The theory of interest*. Macmillan.

Frank, M. Z., & Shen, T. (2016). Investment and the weighted average cost of capital. *Journal of Financial Economics*, *119*(2), 300-315. https://doi.org/10.1016/j.jfineco.2015.09.001

Gaspars-Wieloch, H. (2019). Project Net Present Value estimation under uncertainty. *Central European Journal of Operations Research*, *27*, 179-197. https://doi.org/10.1007/s10100-017-0500-0

Gordon, M. J., & Shapiro, E. (1956). Capital Equipment Analysis: The Required Rate of Profit. *Management Science*, *3*(1), 102-110. https://doi.org/10.1287/mnsc.3.1.102

Kari, M. J., & Pynnöniemi, K. (2019). Theory of strategic culture: An analytical framework for Russian cyber threat perception. *Journal of Strategic Studies*, 1-29. https://doi.org/10.1080/01402390.2019.1663411

Kazlauskienė, V. (2015). Application of Social Discount Rate for Assessment of Public Investment Projects. *Procedia - Social and Behavioral Sciences*, *213*, 461-467. https://doi.org/10.1016/j.sbspro.2015.11.434

Kossova, T., & Sheluntcova, M. (2016). Evaluating performance of public sector projects in Russia: The choice of a social discount rate. *International Journal of Project Management*, *34*(3), 403-411. https://doi.org/10.1016/j.ijproman.2015.11.005

Kuehl, D. T. (2009). From Cyberspace to Cyberpower: Defining the Problem. In *Cyberpower and National Security* (pp. 24-42). Potomac Books and National Defense University. https://doi.org/10.2307/j.ctt1djmhj1.7

Macrotrends. (2023). *Russia Inflation Rate 1993-2023*. Retrieved from https://www.macrotrends.net/countries/RUS/russia/inflation-rate-cpi

Manky, D. (2013). Cybercrime as a service: A very modern business. *Computer Fraud and Security*, *2013*(6), 9-13. https://doi.org/10.1016/S1361-3723(13)70053-8

Miller, C. (2010). Kim Jong-il and me: How to build a cyber army to attack the U.S. *DEF CON 18*. Retrieved from https://defcon.org/images/defcon-18/dc-18-presentations/Miller/DEFCON-18-Miller-Cyberwar.pdf

Moore, M. A., Boardman, A. E., Vining, A. R., Weimer, D. L., & Greenberg, D. H. (2004). Just give me a number! Practical values for the social discount rate. *Journal of Policy Analysis and Management*, *23*(4), 789-812. https://doi.org/10.1002/pam.20047

Myers, S. C. (1974). Interactions of Corporate Financing and Investment Decisions-Implications for Capital Budgeting. *The Journal of Finance*, *29*(1), 1-25. https://doi.org/10.2307/2978211

OASIS. (2021). *STIX Version 2.1*. Retrieved from https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html

Paganini, P. (2022). *Experts analyzed the evolution of the Emotet supply chain*. Retrieved from https://securityaffairs.co/136935/malware/emotet-evolution-ttps.html

Proofpoint. (2019). *Threat Actor Profile: TA542, From Banker to Malware Distribution Service*. Retrieved from https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta542-banker-malware-distribution-service

Ramsey, F. P. (1928). A Mathematical Theory of Saving. *The Economic Journal*, *38*(152), 543-559. https://doi.org/10.2307/2224098

Sharpe, W. F. (1964). Capital asset prices: A theory of market equilibrium under conditions of risk. *The Journal of Finance*, *19*(3), 425-442. https://doi.org/10.1111/j.1540-6261.1964.tb02865.x

Sun, W., Ding, Z., & Xu, X. (2021). A new look at returns of information technology: firms' diversification to IT service market and firm value. *Information Technology and Management*, *22*(1), 13-31. https://doi.org/10.1007/s10799-021-00322-y

Szőr, P. (2005). *The Art of Computer Virus Research and Defense*. Pearson Education (US).

Theocharidou, M., Malatras, A., Lella, I., & Tsekmezoglou, E. (2021). *Threat Landscape 2021*. ENISA. https://doi.org/10.2824/324797

Tudor, D. (2022, March 22). *Malware as a Service (MaaS). What It Is and How It Can Threaten Your Business?* Heimdal Security. Retrieved from https://heimdalsecurity.com/blog/what-is-malware-as-a-service-maas/

WageIndicator Foundation. (2023). *Minimum Wage – Russia*. Retrieved from https://wageindicator.org/salary/minimum-wage/russia

Zhuang, J., Liang, Z., Lin, T., & xDe Guzman, F. D. (2007). *Theory and practice in the choice of social discount rate for cost-benefit analysis: A survey*. Retrieved from http://hdl.handle.net/11540/1853