Hindawi
Security and Communication Networks
Volume 2022, Article ID 5784674, 11 pages
https://doi.org/10.1155/2022/5784674

Research Article

Identifying Key Relationships between Nation-State Cyberattacks and Geopolitical and Economic Factors: A Model

Lorena González-Manzano,[1] **José M. de Fuentes**,[1] **Cristina Ramos**,[1] **Ángel Sánchez**,[2] **and Florabel Quispe**[3]

[1]*Computer Security Lab (COSEC), Department of Computer Science and Engineering, Universidad Carlos III de Madrid, Madrid 28911, Spain*
[2]*Department of Mathematics, Universidad Carlos III de Madrid, Madrid 28911, Spain*
[3]*Department of International Law, Ecclesiastical Law and Philosophy of Law, Universidad Carlos III de Madrid, Madrid 28911, Spain*

Correspondence should be addressed to Lorena González-Manzano; lgmanzan@inf.uc3m.es

Received 8 October 2021; Revised 23 February 2022; Accepted 8 June 2022; Published 29 June 2022

Academic Editor: Konstantinos Rantos

Nation-state cyberattacks, and particularly Advanced Persistent Threats (APTs), have rocketed in the last years. Their use may be aligned with nation-state geopolitical and economic (GPE) interests, which are key for the underlying international relations (IRs). However, the interdependency between APTs and GPE (and thus IRs) has not been characterized yet and it could be a steppingstone for an enhanced cyberthreat intelligence (CTI). To address this limitation, a set of analytic models are proposed in this work. They are built considering 234M geopolitical events and 306 malicious software tools linked to 13 groups of 7 countries between 2000 and 2019. Models show a substantial support for launched and received cyberattacks considering GPE factors in most countries. Moreover, strategic issues are the key motivator when launching APTs. Therefore, from the CTI perspective, our results show that there is a likely *cause-effect relationship* between IRs (particularly GPE relevant indicators) and APTs.

1. Introduction

Cyberthreats have been on the rise in the last years, with cyberthreat intelligence (CTI) being a key subject to mitigate damage in the cyberspace. According to the latest EUROPOL's Internet Organized Crime Threat Assessment, cybercriminals have evolved their modus operandi to improve their success rate [1]. As such, the World Economic Forum has identified cyberattacks as the greatest non-environmental threat to humanity [2].

Beyond traditional malwares (e.g., ransomware, trojans, etc.), a particular set of advanced threats are also increasing: Advanced Persistent Threats (APTs). APTs are typically carried out by powerful actors which count on substantial resources to build a long-lasting malware [3]. Although the attribution is typically cumbersome, it is generally accepted that most of the APTs are state-sponsored. For example, CozyDuke APT is allegedly linked to the Russian-based APT29 group [4]. As opposed to regular malwares, APTs are usually focused on stealing information or compromising devices. They have already been applied against other countries or opponents, such as the case of Chinese APTs against Tibetan organizations [5].

The relationship between targeted cyberattacks and international relations (IRs) has already been pointed out. From a CTI perspective, it is quite useful for a better understanding of a particular incident. Particularly, the influence of geopolitical and economic issues (hereinafter, GPE) has been identified in concrete events [6, 7]. These cyberattacks may be human- or computer-focused. As an example of the first case, the recent COVID-19 pandemic has led to a substantial amount of disinformation campaigns [8]. However, computer-focused attacks have been at stake for a longer period and thus they are at the core of this paper. For example, a large-scale distributed denial of service attack was launched by Russia over Estonia because of the latter moving a Soviet-era statue (Geers [9]). Overall, cyberattacks tied to cyberwars, or geopolitical conflicts, increased from 19% in 2018 to 27% in 2019 [10]. This has also led to some political agreements on the use of cyberspace. For example, China and Russia signed in 2015 an agreement on "cooperation in ensuring international information security" [11]. Despite the agreement, Russian-related APTs have been launched against China after that date.

The implications of the use of cyberspace to impact other countries have already been highlighted, even from the main actors. In this regard, China and Russia asked for an "international code of conduct for information security" back in 2011 [12]. In the same line, China stated in 2017 that "no country should pursue cyberhegemony, interfere in other countries' internal affairs, or engage in, condone, or support cyberactivities that undermine other countries' national security." Despite these political statements, both China and Russia have been linked to a vast number of APTs against other countries. This trend has been followed by several other nations around the world. According to FireEye, countries such as Iran, Vietnam, or North Korea are among the most prominent ones [13]. Indeed, public attribution of cyberattacks has also been studied considering its political implications [14]. This particular feature calls for a potential *mutual influence* of IR (particularly GPE issues) and nation-state cyberattacks (APTs), which has been long studied. From a broader perspective, geopolitics has already been pointed out as an influencer for cyberattacks [15, 16]. With a closer focus, socioeconomic, psychosocial, and geopolitical factors of cybercrime are analysed in [17], being particularized in Nigeria. However, to the best of the authors' knowledge, this influence has not been empirically measured. Indeed, this problem cannot be addressed from the computer science or the IRs perspectives alone; an interdisciplinary approach is needed.

To overcome this limitation, in this paper, we aim to build a set of analytical models to determine the strength of the relationship between APTs and GPE matters, thus shedding light on a CTI process. For the sake of relevance, the models will be applied considering 13 of the most active APT groups according to the Thales-Verint index [18] and FireEye [13]. This results in 7 attacker countries and 6 victim ones.

This paper tackles two research questions, leading to the following contributions.

RQ1. Are there (possibly causal) relationships between GPE issues and APTs worldwide? Do such relationships hold for a given region or country?

(i) We provide a mathematical characterization of the relevance of this relationship.

(ii) We analyse this matter for attacks carried out and received by the United States, Russia, China, Iran, India, Vietnam, and North Korea, as they are linked to the most relevant APT groups worldwide.

RQ2. Which are the underlying motivations for each attacking country?

(i) We analyse the individual relevance of three GPE factors, namely, economical, strategical, and warfare motivators on launching APT-based cyberattacks. This allows characterizing the alignment of APTs with the national strategy of the attacking country, which has been pointed out as an open research issue [19].

This paper is structured as follows. Section 2 analyses related works. Afterwards, Section 3 introduces the background and describes the applied methodology. Section 4 presents results. Lastly, Section 5 concludes the paper and points out future research directions.

2. Related Works

In the last 10 years, in the CTI context, many efforts have been made to analyse APTs. From a technical perspective, MITRE corporation has developed MITRE ATT&CK, a repository of attacks and techniques [20]. In this project, groups of attacks are linked to APTs and their purported origins, leading to MITRE Groups catalogue. At academic level, [21, 22] studied multiple APTs in terms of their deployment and evolution, from the initial system compromise to its control. By contrast, [23] analysed some common attack methods and tools used by APTs, while [24] studied behaviours of multiple APTs and their protection measures. Reference [25] presented a deeper analysis, identifying APTs in which actors, type, and content can be deduced. Moreover, [26] developed a survey on APTs, presenting a systematic review of their methods and techniques, as well as methods for their detection.

From a sociopolitical perspective, several years ago, in 1998, [27] searched for a cause-and-effect model of attacks on information systems, called cyberattacks nowadays. Later, [28] presented a theoretical study of a subset of cyberattacks, from 1995 to 2009, with political, sociocultural, and economic motivation. Although they are not related to APTs, it is pointed out that cyberattacks are strongly correlated to political and cultural conflicts. Similarly, but without a clear link to cyberattacks, [29] presented a theoretical discussion towards political, technological, and scientific factors in terms of cybersecurity politics. Moreover, [30] considered cyberattacks as social events associated with social, political, economic, and cultural (SPEC) factors to understand the motivations behind them. In particular, the correlation of variables and network analysis is used to assess the relevance of factors such as corruption and the income difference. Just in the social dimension, [31] analysed cyberattacks to build a threat model based on past and current social events through a Formal Concept Analysis (FCA) approach and a Fact Proposition Space (FPS) inference technique. Knowledge is acquired from news articles and the evaluation is carried out over 14 news articles linked to some cyberattacks from 1995 to 2010.

On the other hand, without mentioning APTs, but using the term state-sponsored cyberattacks, [32] analysed incidents of such attacks regarding intra- and interindustry trade. The evaluation of the proposal involves variables such as cyberespionage campaigns, information about trade data, GDP per capita, or conflict data. In a more recent approach, [33] presented a GPE analysis to cover which countries strategic motivations are in line with the observed attacker activity from an APT attribution perspective. Who benefits from the attacks is discussed, pointing out political and economic interests but in a general way and without focus on APTs. Last but not least, [34] used event data and a proprietary cyberincident dataset to investigate what happens between countries when cyberconflict is used in foreign policy interactions. It is found that only distributed denial of service attacks affect relationships between states, as well as the change of political behaviour and policies.

Table 1 presents an analysis of existing CTI approaches related to the presented proposal. It points out if they deal with APTs; if they handle, discuss, or analyse GPE factors; if they address any of our proposed research questions; and, finally, the applied methodology and dataset. In light of existing studies, some of them focus on APTs and some other on social or sociopolitical matters related to cyberattacks, but no proposal has modelled and analysed relationships between APTs and GPE concerns. Moreover, in terms of methodology, [32] is the only proposal that applies regression models as in our proposal (introduced later in Section 3.2). However, their models are different as they are used for different purposes. Finally, considering datasets, most of them focus on cyberattacks in general, not in APTs. Just [32, 34] used a dataset involving some APT but their number is quite limited. As a matter of fact, most of their cyberattacks are already included in our study (see Section 3.2.1 for details on our dataset). Moreover, they do not include information of victims or attacked sectors, which are essential to address our research questions.

3. Materials and Methods

3.1. Background. In this section, three basic notions for this proposal are introduced. In particular, the notion of APT is introduced in Section 3.1.1. Afterwards, the Goldstein scale is presented in Section 3.1.2 to rate sociopolitical events. Lastly, linear models required to build the analytical model are described in Section 3.1.3.

3.1.1. APT Concepts. An APT is a sophisticated long-term attack launched against a specific targeted entity [35]. Although attribution is not straightforward, researchers agree that these types of attacks are usually coordinated by highly specialized and skilled teams, usually funded by (or linked to) governments or nation states (hereafter referred to as APT groups) [36]. Each APT group materialises its cyberattacks in the form of campaigns, and each campaign has a set of technical indicators associated with it, such as start and end dates, Software Tools (STs), and victims. In this paper, the amount of cyberattacks (sent or received) has been measured by the number of STs in use per year. For example, the Chinese APT group called APT10 developed the "menuPass" campaign with 3 used STs in 2016, namely, ChChes, PlugX, and Poison Ivy [37]. We adopt this indicator as it is clearly stated in all considered reports. Indeed, although the number of victims could also be taken into account, some of them could not be known and this would have a negative impact on the robustness of the data at stake.

3.1.2. Rating Geopolitical Events: The Goldstein Scale. Conflict and Mediation Event Observations (CAMEO) is a taxonomy for coding event data [38]. It was developed to correct some of the problems in the WEIS (World Event Interaction Survey) and the COPDAB (Conflict and Peace Data Bank) coding systems [38]. For each event, an indicator of its intensity is given following the Goldstein scale. It assigns a numerical score between −10 (the most conflictual event) and +10 (the most cooperative one), capturing the theoretical potential impact that type of event will have on the stability of a country.

3.1.3. Linear Models. To analyse the relationship between GPE issues and APTs, multiple linear regression models [39] are used. In a nutshell, in these models, the predicted scalar magnitude Y is assumed to depend on several explanatory variables x_i (see Equation (1)). This dependence is assumed to be linear and the weight β_i for each explanatory variable is estimated from the data. This procedure will allow us to understand how the variation in the predicted variable is related to the variation in the explanatory variables. As this does not usually lead to a perfect fit, a negligible factor ϵ is typically needed. As usual, the explanatory power will be characterized by the adjusted R^2 coefficient (in the range $[-1, 1]$) which is the amount of variation explained.

$$Y = \beta_0 + \beta_1 x_1 + \beta_2 x_2 + \beta_3 x_3 + \varepsilon. \quad (1)$$

3.2. Methodology. The proposed research questions are answered based on a methodology composed of the steps highlighted in grey in Figure 1. Data is collected in first place (Section 3.2.1), identifying cyberattacks (Section 3.2.1(1)), and GPE factors (Section 3.2.1(2)), to generate models afterwards (Section 3.2.2). Moreover, for consistency purposes and to ensure the validity of the models, the alignment between attacked sectors and cyberattack motivations is also analysed (Section 4.2).

3.2.1. Source Data Collection. Data is collected for all studied countries and distinguishing, when required, between attackers and victims. The following sections describe the nature of the data used in the models' construction. To foster further research in this area, our dataset has been publicly released in GitHub (https://github.com/crramosi/APTs-Dataset).

(1) Cyberattacks. This research is based on 13 of the most relevant APT groups attributed to 7 different countries according to the Cyberthreat Handbook by Thales-Verint [18] and FireEye [13] (see Table 2). Our selection promotes that significant APT groups are considered and that regional

Table 1: Related work analysis.

	APTs	GPE factors	RQ1	RQ2	Methodology	Dataset
[27]	x	√	x	x	Custom cause-and-effect model	Custom set of attacks, actors, and defenses
[28]	x	√	x	x	Theoretical	31 cyberattacks
[29]	x	√	x	x	Theoretical	Theoretical
[30]	x	√	x	√	Pearson's correlation and quadratic assignment procedure	Arbor Networks DDoS attacks data, World Bank Open Data, EconStats web page, and U.S. Naval Academy data
[31]	x	√	x	x	Formal Concept Analysis	Open resources such as online news articles, books, and scholarly journals and papers
[32]	√	√	x	x	Baseline logistic regression models, mixed-effects models, and rare events logistic models	Dyadic Cyber Incident and Campaign Dataset version 1.5, Standard International Trade Classification level 5, World Development Indicators, Economic Complexity Index from the MIT's Observatory of Economic Complexity, Idealpoint index, Polity IV Project, and UCDP/PRIO Armed Conflict Dataset
[33]	√	√	x	x	Theoretical	Theoretical
[34]	√[1]	√[2]	x	x	Ordinary Least Squares fixed-effects models and Generalised Least Squares (GLS) random-effects models	Dyadic Cyber Incident and Dispute Dataset version 1.0 and media sources
Ours	√	√	√	√	Linear regression models	13 APT groups, GDELT data, World Development Indicators database, the United Nations Statistics Division, and the International Monetary Fund

[1] Not only APTs but also a more diverse set of cyberattacks are considered. [2] Only strategic/diplomatic factors are considered.

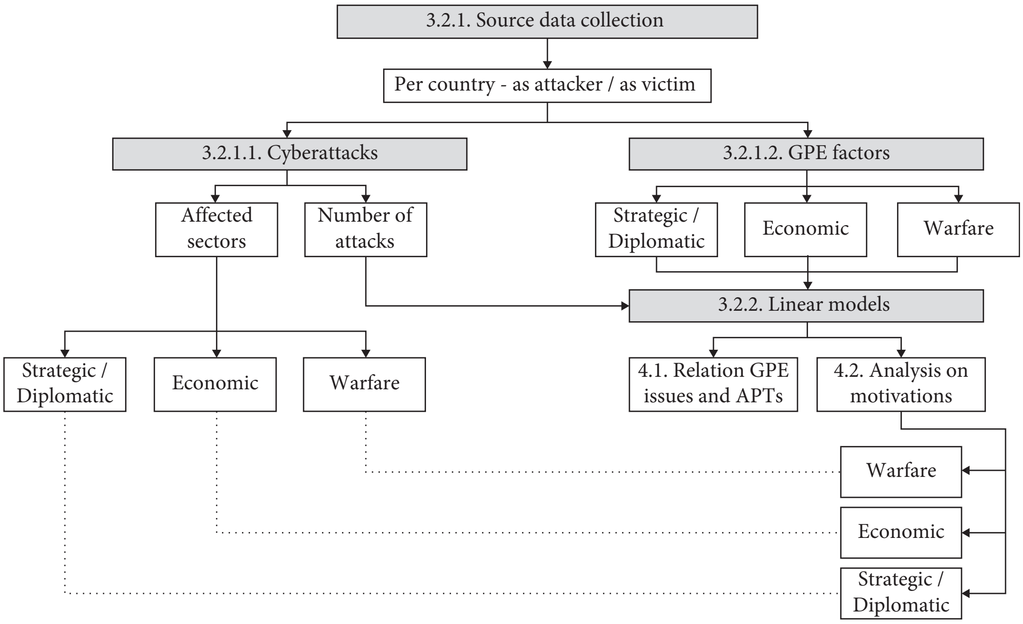

Figure 1: Methodological scheme.

diversity is preserved. In total, 439 different reports, publications, and blog entries have been studied, which describe 306 STs. All sources are public and freely accessible, including cybersecurity firms and vendors such as Kaspersky [53], the United States (US) Cybersecurity and Infrastructure Security Agency (CISA) [54], collaborative platforms such as Malpedia [55], and cybersecurity blogs such as Security Affairs [56].

The process of collecting cyberattacks was carried out in line with [57] to generate a reliable and quality dataset; cyberattacks were collected from the relevant set of sources cited beforehand. At the beginning, any cyberattack that could be considered an APT attack was collected, whether it met the exact definition or not. Once all cyberattacks were collected, it was decided whether they met the APT definition by a text search for keywords such as group name and aliases. Moreover, a test-retest method has been applied in this process; all data were initially encoded according to a coding manual (available in GitHub repository), and this process was repeated

Table 2: Summary of APT groups and considered reports.

APT group	Presumed origin country	STs	Studied reports
APT29 [40]	Russia	24	48
APT10 [41]	China	30	34
APT28 [42]	Russia	24	95
APT35 [43]	Iran	16	26
Equation [44]	United States	7	12
APT38 [45]	North Korea	33	36
APT32 [46]	Vietnam	31	27
Lazarus [47]	North Korea	93	69
APT12 [48]	China	7	12
Patchwork [49]	India	11	17
BeagleBoyz [50]	North Korea	10	21
APT33 [51]	Iran	20	45
Dark basin [52]	India	0	7

some months later to ensure the reliability and quality of the data at stake.

Most of the studied STs are from North Korea (136), followed by Russia (48), China (37), Iran (36), Vietnam (31), India (11), and USA (7). It must be noted that one APT group called Dark Basin has not created any ST according to existing reports due to its novelty. However, the considered reports describe recent cyberattacks against different victims and sectors. Thus, even if there is no mention to the associated STs, this group is kept for the sake of completeness.

Gathering APT groups based on the presumed origin country, we studied cyberattacks either as attacker or as victim in China (CHN), India (IND), Iran (IRN), North Korea (PRK), Russia (RUS), United States (USA), and Vietnam (VNM). Considering the selected reports, technical data on their campaigns have been obtained for each group, including (when possible) start and end dates, used STs and victim sectors, and countries (available in GitHub repository). For illustrative purposes, Table 3 presents a summary of the number of uses of STs that each country has made (as attacker) or suffered (as victim). It must be noted that each ST may be used several times and that a given country may use STs from another one. Thus, the amount of STs created (Table 2) and that of ST uses (Table 3) do not necessarily match.

The collected data shows that RUS and PRK are the most active countries and that USA is by far the most targeted country, with more than 180 cases. No data is known for PRK as victim, as it has not been publicly disclosed.

(2) GPE Factors. We differentiate three main factors within GPE issues, namely, strategic/diplomatic, economic, and warfare. Considering the influence of geopolitical and economic issues in cyberattacks (recall Section 1), although the potential motivation for a cyberattack may be diverse, it has been pointed out that GPE factors are the usual ones [58]. Indeed, as pointed out in Section 2, several works deal with them. Concerning the first type, conflicts and agreements between countries are retrieved using the GDELT database. GDELT is a free, global, open-source project that monitors radio, press, and web news from around the world in real time and converts them into a common format for open research, thus breaking down language and access barriers and becoming a valuable data source [59]. In particular, the GDELT Event Database collects daily the physical activities (or events) described in the news. In addition, it uses the CAMEO event taxonomy in its latest version (recall Section 3.1.2), capturing two actors and the action (event) performed by *Actor1* upon *Actor2*. It offers a wide range of features including the Goldstein scale and number of mentions, that is, the total number of citations of each event across all source documents. Relying upon GDELT is beneficial as it gathers the information surrounding political conflicts in a continuous manner, so we do not only consider discrete situations which could be scarce. In total, 234,080,914 events were studied related to the period between 2000 and 2019 (see Table 4).

To measure the relevance of each event, the Goldstein score (recall Section 3.1.2) is used as an approximation of the impact of that event. With this scale, it is possible to define whether relations between countries are bad (negative values) or good (positive values). To get a precise measurement, it must be noted that each event in GDELT can have one or more appearances (subEvents). Each subEvent has also a number of mentions, which reflect their relevance in terms of media coverage. Thus, two strategic or diplomatic variables have been created, *PositiveValue* and *NegativeValue*, calculated per year as the sum of all events as follows:

$$\begin{aligned}\text{PositiveValue} = \sum (\text{NumberSubEvents} * \text{MeanMentions} * \text{GoldsteinScore})\\ \text{where Goldstein Score} > = 0,\end{aligned} \tag{2}$$

$$\begin{aligned}\text{NegativeValue} = \sum (\text{NumberSubEvents} * \text{MeanMentions} * \text{GoldsteinScore})\\ \text{where Goldstein Score} < 0.\end{aligned} \tag{3}$$

For each studied year, these formulas classify conflicts (NegativeValue) as events with scores on the Goldstein scale between [−10, 0) and agreements (PositiveValue) as events with scores on the Goldstein scale between [0, +10]. In addition, they multiply events by their average number of mentions (MeanMentions) as a method of assessing the importance of the event. Thus, the

Table 3: Summary of used STs per country as attacker or victim.

Country	Uses of STs (as attacker)	Received STs (as victim)
CHN	92	63
IND	30	81
IRN	84	43
PRK	222	–
RUS	214	51
USA	21	187
VNM	82	26

Table 4: Summary of considered GDELT events.

Country	Number of events as attacker	Number of events as victim
CHN	10,183,203	8,657,367
IND	5,071,275	3,507,981
IRN	5,929,306	5,337,900
PRK	1,966,712	1,901,801
RUS	10,066,365	8,578,279
USA	98,251,628	71,746,718
VNM	1,541,431	1,340,948

combination of the amount of appearances, their media relevance, and the event nature measures the significance of each event for the relationship between a pair of countries.

With respect to economic motivations, we consider data provided by the World Development Indicators database [60], the United Nations Statistics Division [61], and the International Monetary Fund [62]. In particular, four indicators are considered, namely, the Human Development Index (HDI), the Gross Domestic Product Per Capita (GDP_PC), the amount of exports and imports (ExportsImports), and the foreign direct investment (ForeignDirectInvestmentNetInflows). They collectively provide a simplified vision of the status of a country from a macroeconomic perspective. The latter refers to the sum of equity capital, reinvestment of earnings, other long-term capital, and short-term capital and measures the interest of third parties into a given country. It must be noted that not all indicators are provided on a yearly basis. Thus, GDP_PC, ExportsImports, and ForeignDirectInvestmentNetInflows range from 2000 to 2010 in five-year jumps and from 2010 to 2019 in annual jumps. To manage this issue, the five-year gaps are filled with progressive values (e.g., if GDP_PC is 1,000 in the year 2000 and 2,000 in 2005, 2006 is assumed to be 1,200, 2007 would be 1,400, and so on) and the annual gaps are filled with the average of the adjacent values.

Last but not least, indicators of warfare motivations are those related to military expenses (MilitaryExpenditure), retrieved from the World Development Indicators database [60] and in line with related works (recall Section 2). It includes current and capital expenditures of the armed forces, defense ministries and other government agencies, paramilitary forces, and military space activities. In this case, data is again not provided on a yearly basis and the same approach as for economic features' annual gaps has been applied.

3.2.2. Linear Models. The final step is the identification of relationships between GPE issues and APTs, which is achieved by computing linear models based on data from each victim/attacked country. Models are developed based on Equation (4), where G, P, and E are GPE factors, and the predicted variable is the amount of STs. In this way, CTI can benefit from this analysis by understanding the relationship between cyberattacks and GPE factors, thus answering RQ1.

$$ST = \beta_0 + \beta_1 G + \beta_2 P + \beta_3 E + \varepsilon. \tag{4}$$

Besides, the motivations of cyberattacks and affected sectors are identified to answer RQ2. This is also useful to assess the consistency of the previous model, as GPE factors and sectors at stake should be aligned. For example, if economic issues are the most prominent GPE factor, it should be more reasonable to attack the financial sector rather than nursery schools. Similarly, defense-related institutions can be regarded as a means to conduct cyberwars. A taxonomy of sectors and their related motivations has been applied (available in GitHub repository). Considering these factors, the analysis of motivations is carried out except for North Korea, as it does not disclose any economic or warfare indicator.

4. Results and Discussion

Leveraging collected data, models to study the relationship between GPE issues and used STs are introduced in this section. Depending on the target relationship, the whole set of countries or a subset of them come into play. As a result, the model selects the variables that better explain cyberattacks, that is, maximizing the adjusted R^2.

The relationship between GPE issues and cyberattacks, related to RQ1, is addressed in Section 4.1. Afterwards, the underlying motivations related to RQ2 are introduced in Section 4.2. Lastly, a summary of the results and the limitations of the work are discussed in Section 4.3.

4.1. Relationship between GPE Issues and Cyberattacks. Tables 5 and 6 present a summary of the developed models for each country as attacker or victim, respectively.

In general terms, the model shows a substantial support for launched cyberattacks considering GPE factors in most countries. As such, cyberattacks from RUS, IRN, and USA count on the highest support. It must be noted that the case of RUS is noteworthy, since the amount of used STs is quite extensive with more than 200 cases.

The situation is even better in terms of the received cyberattacks. Our results show that the considered factors provide with great support. Interestingly, USA has received more than 180 cyberattacks and the model supports them with a factor of 0.82. On the other side, the lowest support is for the attacks received by IRN. However, it is an exception, since the remaining countries are beyond 0.7.

4.2. Analysis on Motivations. The following sections study motivations of cyberattacks per country, including a consistency analysis, as well as devising motivations per attacker on each victim.

Table 5: Relationship analysis (attacker perspective).

Country	Final variable/s	Adjusted R^2
CHN	HDI, GDP_PC, ForeignDirectInvestmentNetInflows	0.55
IND	HDI, GDP_PC, ExportsImports	0.55
IRN	PositiveValue, NegativeValue, HDI, GDP_PC, ExportsImports, ForeignDirectInvestmentNetInflows	0.68
PRK	PositiveValue, NegativeValue	0.48
RUS	PositiveValue, NegativeValue, GDP_PC, ExportsImports, ForeignDirectInvestmentNetInflows, MilitaryExpenditure	0.94
USA	HDI, GDP_PC, ExportsImports, ForeignDirectInvestmentNetInflows	0.63
VNM	PositiveValue, HDI, GDP_PC, ExportsImports	0.60

Table 6: Relationship analysis (victim perspective).

Country	Final variable/s	Adjusted R^2
CHN	PositiveValue, NegativeValue, HDI, ExportsImports, ForeignDirectInvestmentNetInflows	0.78
IND	PositiveValue, NegativeValue, HDI, GDP_PC, ForeignDirectInvestmentNetInflows, MilitaryExpenditure	0.79
IRN	NegativeValue, HDI, GDP_PC, ExportsImports, ForeignDirectInvestmentNetInflows, MilitaryExpenditure	0.42
RUS	NegativeValue, HDI, ExportsImports, ForeignDirectInvestmentNetInflows, MilitaryExpenditure	0.77
USA	PositiveValue, NegativeValue, HDI, GDP_PC, ExportsImports	0.82
VNM	PositiveValue, HDI, GDP_PC, ForeignDirectInvestmentNetInflows, MilitaryExpenditure	0.92

4.2.1. Motivations per Country. In order to understand the relevance of each motivation per country, a linear model is built by only considering the variables related to each GPE factor (recall Section 3.2.1(2)). Table 7 summarizes results considering all countries. In general terms, most countries show strong prevalence of strategic and economic issues when launching cyberattacks. Indeed, China and Russia achieve similar support rates in both matters. The case of Russia is in line with prior expectations [58]. Similarly, Iranian STs have also been aligned with strategic issues as their main focus is on domestic regime stability [63]. On the contrary, Chinese STs have been regarded as more economic-driven in support of the country's five-year plan [64].

Last but not least, warfare issues are not relevant for most countries except from Russia and USA as attackers and Vietnam as victim. The most notable result is Russia as attacker, which is probably because one of its most noteworthy APT groups is linked to a military intelligence service [65]. Similarly, the warfare interest of USA might be explained by considering that its APT group (called Equation) is allegedly linked to the US National Security Agency.

4.2.2. Consistency Analysis on Motivations. To further confirm the strength of these motivations, victim sectors are also considered. It is expected that the choice of target sectors is also aligned with the pinpointed GPE sectors.

Based on studied reports, Table 8 presents the percentage of sectors in which each country has been attacker or victim. Most target sectors are strategic or diplomatic, followed by economic ones. Regarding the warfare sectors, results show their lower relevance. However, all countries have attacked or have been victims in cyberwar-related sectors at some point.

The consistency analysis is carried out based on the alignment between the number of targeted sectors and the models previously developed (recall Table 7). If the corresponding percentage of attacks for a particular GPE factor is the highest one and the model also reveals the highest R^2 for such GPE factor, there is an alignment between both. The study reveals that there is a close relationship between economic and strategic variables, though, in many cases, the alignment is achieved. For instance, IRN has a 0.58 in the model as an attacker (Table 7) for strategic/diplomatic variables, and the results by sector (Table 8) show that IRN attacks more sectors within that category (57.01%). This is in line with prior works [66, 67] which point out IRN's prevalent strategic interest, or VNM's focus on strategy but with substantial economic interests [68]. Indeed, from the attacker perspective, CHN, USA, and RUS are the exceptions, because our model suggests an economic motivation in first place, while sectors point out a higher strategic one. Concerning CHN, it is interested in increasing its technological level through industrial espionage and thus increasing its economical position [69]. Moreover, economy is a priority in USA, though strategic issues are also an important matter [70]. Lastly, the case of RUS is surprising for the low prevalence of economic sectors. However, Russian cyberattacks are launched against other states with preexistent rivalry [71] and thus strategic/diplomatic issues as pointed out by the model.

Concerning the victims' perspective, results are consistent except for IRN, RUS, and VNM; the model points out that the main motivation is economy, but the targeted sectors are mainly strategic in nature. Nonetheless, in line with the model, the relevance of economic sectors is notorious in these cases, so it may represent that their attackers are aiming to steal information from economy-unrelated sectors that can later be transformed into economical assets.

4.2.3. Motivations per Attacker on Each Victim. To complete the analysis of the motivations for each country, it is also necessary to study their attacks against other target

Table 7: Influence of each GPE factor per country as attacker/victim.

Country	Economy adjusted R^2	Strategy or diplomacy adjusted R^2	Warfare adjusted R^2
Attacker perspective			
CHN	0.55	0.51	0.06
IND	0.46	0.55	0.17
IRN	0.43	0.58	−0.06
PRK	—	0.48	—
RUS	0.89	0.81	0.64
USA	0.64	0.44	0.49
VNM	0.28	0.51	0.12
Victim perspective			
CHN	0.60	0.65	0.08
IND	0.036	0.58	0.07
IRN	0.33	0.14	−0.03
PRK	—	—	—
RUS	0.73	0.56	0.10
USA	0.76	0.80	0.02
VNM	0.88	0.85	0.33

Table 8: Targeted sectors per country as attacker/victim.

Country	Economy	Strategy or diplomacy	Warfare
Attacker perspective			
CHN	45.61%	52.98%	1.40%
IND	43.06%	54.34%	2.60%
IRN	39.25%	57.01%	3.74%
PRK	34.11%	45.31%	20.57%
RUS	24.31%	66.30%	9.39%
USA	40.00%	55.00%	5.00%
VNM	45.74%	53.19%	1.06%
Victim perspective			
CHN	41.82%	54.38%	3.79%
IND	43.79%	54.09%	2.12%
IRN	40.95%	53.78%	5.27%
PRK	—	—	—
RUS	41.78%	54.46%	3.76%
USA	9.57%	55.61%	4.82%
VNM	44.44%	53.70%	1.85%

countries. For this purpose, models are developed for pairs of attackers and victims. Results are presented in Table 9, where suffixes C1 and C2 represent attacker and victim-related variables, respectively. For the sake of soundness, only those attacker-victim pairs with more than 15 used STs have been considered.

On the one hand, the situation between IND and CHN has recently been highlighted, although their tensions have arisen from a long time now [72]. Our results show that there is some support between GPE issues and cyberattacks in their case. On the other hand, it is noteworthy that all studied countries attack USA, and most of them count on remarkable support considering the GPE factors. USA itself already pointed out that CHN, RUS, and IRN were among the three main actors that were leveraging STs for cyber-espionage with economic interests [73]. Our results show that though strategic factors seem to prevail, economic issues are at stake in most countries. This is consistent with the previous models (recall Tables 7 and 8).

4.3. Summary and Limitations. In light of the results achieved from the models, and in line with the research questions, it can be concluded that there is an undeniable relationship between GPE factors and cyberattacks (RQ1). Moreover, it has been shown that strategic issues are the most relevant GPE factor to launch cyberattacks but very close to the economic ones (RQ2). Our results are mostly in line with prior works that addressed the motivation for studied countries.

Beyond qualitative statements of motivation of APTs, which are quite common (e.g., Threat Group Cards produced by Thailand's Computer Emergency Response Team [74]), our work is the first in providing quantitative measurements in this regard. This is beneficial for CTI for two reasons. The first reason is that it expands the horizon when it comes to solving the attribution of a cyberattack; GPE factors may serve as a hint to differentiate between different candidate attackers. The second reason is that monitoring GPE factors may be helpful to better predict future APT-related cyberattacks.

Despite the relevance of these results, it must be noted that our findings may be limited for several reasons. On the one hand, only a subset of the most representative APT groups have been analysed. Therefore, cyberattacks launched by other groups could alter the results.

A second limitation is related to the number of countries at stake. Our sample is representative as it covers the most active countries in terms of APT-based cyberattacks. However, the inclusion of additional countries is left for future work. Thirdly, the considered period of activity for each group and the current status of the media coverage as gathered by GDELT may impact the model. Indeed, a sensitivity analysis would be beneficial to assess the long-term stability of our findings.

A fourth limitation is related to our consistency analysis. It relies upon a set of sector-motivation associations that have been proposed in this paper. Therefore, different associations (e.g., including secondary motivations) could impact the degree of consistency.

Last but not least, our models do not capture eventual indirect cyberattacks in which a country targets another one by attacking some of the target's allies or when the attack is carried out by a country which acts as proxy of the actual attacker. Nevertheless, including these events could decrease the strength of our model, since the attribution and intent of cyberattacks are not straightforward. Therefore, additional assumptions should be added to determine if a cyberattack was directed against the actual victim or against another third party. In this work, we have opted for sticking to evidence provided by the studied reports. The only assumption taken relies on the connection between sectors and GPE factors, but we believe it is reasonable and it counts on an affordable error margin.

Table 9: Motivation per attacking country and victim.

Attacker country	Victim country	Final variable/s	Adjusted R^2
CHN	IND	PositiveValue, NegativeValue, HDI_C1, HDI_C2, GDP_PC_C1, GDP_PC_C2, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C1, ForeignDirectInvestmentNetInflows_C2, MilitaryExpenditure_C2	0.79
	USA	PositiveValue, NegativeValue, HDI_C1, GDP_PC_C2, ExportsImports_C1, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C1, ForeignDirectInvestmentNetInflows_C2, MilitaryExpenditure_C1	0.44
IND	CHN	NegativeValue, HDI_C1, HDI_C2, GDP_PC_C1	0.41
	USA	PositiveValue, NegativeValue, HDI_C2, GDP_PC_C2, ExportsImports_C1, ForeignDirectInvestmentNetInflows_C2, MilitaryExpenditure_C2	0.84
IRN	USA	PositiveValue, NegativeValue, HDI_C2, GDP_PC_C2, ExportsImports_C1, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C1, ForeignDirectInvestmentNetInflows_C2, MilitaryExpenditure_C1	0.99
PRK	USA	PositiveValue, ExportsImports_C2	0.43
RUS	USA	PositiveValue, HDI_C1, GDP_PC_C2, ExportsImports_C1, ForeignDirectInvestmentNetInflows_C1, ForeignDirectInvestmentNetInflows_C2, MilitaryExpenditure_C1, MilitaryExpenditure_C2	0.86
USA	CHN	PositiveValue, HDI_C1, GDP_PC_C1, GDP_PC_C2, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C1, MilitaryExpenditure_C2	0.72
	IND	NegativeValue, HDI_C1, HDI_C2, GDP_PC_C1, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C2, MilitaryExpenditure_C1, MilitaryExpenditure_C2	0.83
	IRN	PositiveValue, NegativeValue, HDI_C1, GDP_PC_C2, ExportsImports_C1, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C1, MilitaryExpenditure_C1, MilitaryExpenditure_C2	0.76
	RUS	NegativeValue, HDI_C2, GDP_PC_C1, ExportsImports_C1, ExportsImports_C2, ForeignDirectInvestmentNetInflows_C1, MilitaryExpenditure_C1, MilitaryExpenditure_C2	0.66

5. Conclusions

In the last years, the influence of international relations in nation-state cyberattacks has been pointed out. However, this influence has not been previously characterized. Similarly, the underlying intentions for these cyberattacks have been pointed out, but no actual proof on the strength of these attributions has been given. To overcome these limitations, this paper has proposed a method to jointly analyse a particular type of cyberattacks (APTs) and a set of geopolitical and economical (GPE) factors that can be at stake to understand the international relations. We have used linear regression models to identify the relationship between GPE factors and the incidence of APTs, allowing us to identify the key factors related to the existence of such attacks depending on the attacker and the victim. These results, along with the theoretical starting point of the hypotheses that the studied factors are an important driver of APTs discussed in the introduction, allow us to conjecture that there is indeed a relationship between cyberattacks and international relations. This makes sense also in view of the fact that it would be difficult to understand that the relation between factors and APT went in the opposite direction, that is, that APTs drove military expenses or HDI, to name a few. On the other hand, it is hard to point at any possible confounding factor responsible for a noncausal correlation between such variety of indicators and the APTs. Finally, our detailed analyses of each pair of countries involved suggest as well that these cyberattacks can be explained in light of economic, strategic, and cyberwar factors. All these considerations reinforce our conclusion that there is a likely *cause-effect relationship* between international relations (particularly GPE relevant indicators) and APTs. To the best of the authors' knowledge, this is the first work addressing both issues together and, thus, it is a nice tool to help cyberthreat intelligence (CTI) teams in the understanding of studied relationships. Indeed, CTI teams may leverage these results for an enhanced attribution and even prediction of cyberattacks.

A plethora of future works can be devised. For example, our discovered relationship may be the steppingstone to build predictive models leveraging the status of international relations, so that potential cyberattacks may be identified beforehand, being especially useful for cyberthreat intelligence processes. Moreover, our models can be enriched with other remarkable groups. This will also be helpful to determine the long-term stability of the relationship between GPE indicators and APTs. On the other hand, our model may be enriched by considering indirect effects between countries, thus characterizing the influence of the so-called cyberproxies.

Data Availability

Data will be released in GitHub if accepted.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the Madrid Goverment (Comunidad de Madrid-Spain) under the multianual agreement with UC3M ("fostering young doctor research", CAVTIONS-CM-UC3M, DEPROFAKE-CM-UC3M) and in the context of the V PRICIT research and technological innovation regional program; by CAM by grant CYNAMON P2018/TCS-4566-CM, co-funded with ERDF; by Min. of Science and Innovation of Spain by grant ODIO PID2019-111429RB-C21 (AEI/10.13039/501100011033); and by the Spanish Ministerio de Ciencia, Innovación and Universidades-FEDER funds of the European Union support, under project BASIC (PGC2018-098186-B-I00)

References

[1] Europol, *Internet Organized Crime Threat Asessment (IOCTA) 2020*, 2020.

[2] The Editor, *The Cold Cyberwar and Geopolitics: Which Weapons Can Protect Endpoints? 5*, 2020, https://www.watchguard.com/wgrd-news/blog/cold-cyberwar-and-geopolitics-which-weapons-can-protect-endpoints.

[3] NIST, "Computer Security Resource Center," 2021, https://csrc.nist.gov/glossary/term/advanced_persistent_threat#:~:text=Computer%20Security%20Resource%20Center,Projects&text=An%20adversary%20that%20possesses%20sophisticated,cyber%2C%20physical%2C%20and%20deception.

[4] K. Baumgartner and C. Riau, *The CozyDuke APT*, https://securelist.lat/the-cozyduke-apt/76597/June2022, 2015.

[5] M. Raggi, *Chinese APT TA413 Resumes Targeting Of Tibet Following COVID-19 Themed Economic Espionage Campaign Delivering Sepulcher Malware Targeting Europe*, 2020, https://www.proofpoint.com/us/blog/threat-insight/chinese-apt-ta413-resumes-targeting-tibet-following-covid-19-themed-economic.

[6] A. Chiappetta, "The cybersecurity impacts on geopolitics," *Formamente*, vol. XIV, 2019.

[7] K. Kausch, *Cheap Havoc: How Cyber-Geopolitics Will Destabilize the Middle East*, JSTOR, New York, NY, USA, 2017.

[8] D. Steed, *COVID-19: Reaffirming Cyber as a 21st century Geopolitical Battleground*, 2020, https://www.realinstitutoelcano.org/en/analyses/covid-19-reaffirming-cyber-as-a-21st-century-geopolitical-battleground/.

[9] K. Geers, *Cyberspace and the Changing Nature of Warfare*, NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), Estonia, 2008.

[10] O'Malley, *Mike. "Concerned about Nation State Cyberattacks? Here's How to Protect Your Organization*, 2020.

[11] A. Segal, *Peering into the future of sino-russian cyber security cooperation*, 2020, https://warontherocks.com/2020/08/peering-into-the-future-of-sino-russian-cyber-security-cooperation/.

[12] Ministry of Foreign Affairs of the People's Republic of China, *Ministry of Foreign Affairs of the People's Republic of China. China, Russia and Other Countries Submit The Document Of International Code Of Conduct For Information Security To the United Nations*, 2011, https://www.fmprc.gov.cn/mfa_eng/wjb_663304/zzjg_663340/jks_665232/jkxw_665234/201109/t20110914_599206.html.

[13] M. Advanced, *Persistent Threat Groups*, https://www.mandiant.com/resources/apt-groups, 2021.

[14] F. J. Egloff and M. Smeets, "Publicly attributing cyber attacks: a framework," *Journal of Strategic Studies*, pp. 1–32, 2021.

[15] The Recorded Future Team, *Geopolitics: An Overlooked Influencer in Cyber Operations*, https://www.recordedfuture.com/geopolitical-cyber-operations/, 2019.

[16] G. Wood, *Geopolitics and the Digital Domain: How Cyberspace Is Impacting International Security*, 2020.

[17] S. Ibrahim, "Social and contextual taxonomy of cybercrime: socioeconomic theory of Nigerian cybercriminals," *International Journal of Law, Crime and Justice*, vol. 47, pp. 44–57, 2016.

[18] Thales and Verint, *The Cyberthreat Handbook*, 2019.

[19] A. Ahmad, J. Webb, K. C. Desouza, and J. Boorman, "Strategically-motivated advanced persistent threat: definition, process, tactics and a disinformation model of counterattack," *Computers & Security*, vol. 86, pp. 402–418, 2019.

[20] The MITRE Corporation, *Mitre att&ck*, https://attack.mitre.org/, 2021.

[21] M. Ussath, D. Jaeger, F. Cheng, and C. Meinel, "Advanced persistent threats: behind the scenes," in *Proceedings of the 2016 Annual Conference on Information Science and Systems (CISS)*, pp. 181–186, New Jersey, NJ, USA, March 2016.

[22] P. Chen, L. Desmet, and C. Huygens, "A study on advanced persistent threats," in *Proceedings of the IFIP International Conference on Communications and Multimedia Security*, pp. 63–72, Aveiro, Linz, Austria, May 2014.

[23] M. Siddiqi and N. Ghani, "Critical analysis on advanced persistent threats," *International Journal of Computers and Applications*, vol. 141, pp. 46–50, 2016.

[24] I. Jeun, Y. Lee, and D. Won, Tai-hoon Kim, Adrian Stoica, Wai-Chi Fang, and Thanos Vasilakos, "A practical study on advanced persistent threats," in *Computer Applications for Security, Control and System Engineering*, vol. 144-152, Korea, Jeju Island, 2012.

[25] A. Lemay, J. Calvet, F. Menet, and J. M. Fernandez, "Survey of publicly available reports on advanced persistent threat actors," *Computers & Security*, vol. 72, pp. 26–59, 2018.

[26] A. Alshamrani, S. Myneni, A. Chowdhary, and D. Huang, "A survey on advanced persistent threats: techniques, solutions, challenges, and research opportunities," *IEEE Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1851–1877, 2019.

[27] F. Cohen, C. Phillips, L. Painton Swiler et al., "A cause and effect model of attacks on information systems," *Computers & Security*, vol. 17, no. 3, pp. 211–221, 1998.

[28] R. Gandhi, A. Sharma, W. Mahoney, W. Sousan, Q. Zhu, and P. Laplante, "Dimensions of cyber-attacks: cultural, social, economic, and political," *IEEE Technology and Society Magazine*, vol. 30, no. 1, pp. 28–38, 2011.

[29] M. Dunn Cavelty and A. Wenger, "Cyber security meets security politics: complex technology, fragmented politics, and networked science," *Contemporary Security Policy*, vol. 41, no. 1, pp. 5–32, 2019.

[30] S. Kumar and K. M. Carley, "Approaches to understanding the motivations behind cyber attacks," in *Proceedings of the 2016 IEEE Conference on Intelligence and Security Informatics (ISI)*, Tucson, AZ, USA, September 2016.

[31] A. C. Sharma, R. A. Gandhi, William Mahoney, William Sousan, and Q. Zhu, "Building a Social Dimensional Threat Model from Current and Historic Events of Cyber Attacks," in *Proceedings of the 2010 IEEE Second International Conference on Social Computing*, pp. 981–986, Minneapolis, August 2010.

[32] W. Akoto, "International trade and cyber conflict: decomposing the effect of trade on state-sponsored cyber attacks," *Journal of Peace Research*, vol. 58, no. 5, pp. 1083–1097, 2021.

[33] T. Steffens, Timo Steffens, "Geopolitical analysis," in *Attribution of Advanced Persistent Threats: How to Identify the*

Actors behind Cyber-Espionage, vol. 99-116, Berlin, Springer, 2020.

[34] R. C. Maness and B. Valeriano, "The impact of cyber conflict on international interactions," *Armed Forces & Society*, vol. 42, no. 2, pp. 301–323, 2016.

[35] Kaspersky, *What Is An Advanced Persistent Threat (APT)?*, https://www.kaspersky.com/resource-center/definitions/advanced-persistent-threats, 2020.

[36] J. Lake, *What Is an Advanced Persistent Threat (APT), with Examples*, https://www.comparitech.com/blog/information-security/advanced-persistent-threat/, 2020.

[37] J. Miller-Osborn and J. Grunzweig, *MenuPass Returns with New Malware and New Attacks against Japanese Academics and Organizations*, https://unit42.paloaltonetworks.com/unit42-menupass-returns-new-malware-new-attacks-japanese-academics-organizations/, 2017.

[38] P. A. Schrodt, *CAMEO Conflict and Mediation Event Observations Event and Actor Codebook*, http://data.gdeltproject.org/documentation/CAMEO.Manual.1.1b3.pdf, 2012.

[39] D. A. Freedman, *Statistical Models: Theory and Practice*, New Publisher, Berkeley, 2009.

[40] F-Secure, *The Dukes: 7 Years of Russian Cyber-Espionage*, 2015.

[41] FireEye iSight Intelligence, *APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat*, https://www.mandiant.com/resources/apt10-menupass-group, 2017.

[42] FireEye, *APT28 - A Window into Russia's Cyber Espionage Operations?"*, 2014.

[43] C. S. Research Team, *Charming Kitten: Iranian Cyber Espionage against Human Rights Activists*, 2017.

[44] G. R. E. A. T. Kaspersky, *Equation group: questions and answers*, 2015.

[45] T. Haskell, *APT38: Un-usual Suspects*, 2018.

[46] N. Carr, *Cyber Espionage Is Alive and Well: APT32 and the Threat to Global Corporations*, 2017, https://www.mandiant.com/resources/cyber-espionage-apt32#:~:text=Threat%20Research,Cyber%20Espionage%20is%20Alive%20and%20Well%3A%20APT32,the%20Threat%20to%20Global%20Corporations&text=FireEye%20assesses%20that%20APT32%20leverages,aligned%20with%20Vietna.

[47] Novetta, *Operation Blockbuster: Unraveling the Long Thread of the Sony Attack*, 2016.

[48] N. Moran and M. Oppenheim, *Darwin's Favorite APT Group*, https://www.mandiant.com/resources/darwins-favorite-apt-group-2, 2014.

[49] D. Lunghi, J. Horejsi, and C. Pernet, *Untangling the Patchwork Cyberespionage Group*, 2017.

[50] CISA, *FASTCash 2.0: North Korea's BeagleBoyz Robbing Banks*, 2020.

[51] J. O'Leary, J. Kimble, K. Vanderlee, and N. Fraser, *Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and Has Ties to Destructive Malware*, https://www.mandiant.com/resources/apt33-insights-into-iranian-cyber-espionage, 2017.

[52] J. Scott-Railton, H. Adam, B. Abdul Razzak, B. Marczak, S. Anstis, and R. Deibert, *Dark Basin: Uncovering a Massive Hack-For-Hire Operation*, https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/, 2020.

[53] K. Kaspersky, *APT Intelligence Reporting*, https://www.kaspersky.es/enterprise-security/apt-intelligence-reporting, 2021.

[54] Us-Cert, *Cybersecurity and Infrastructure Security Agency*, https://www.cisa.gov/, 2021.

[55] F. K. I. E. Fraunhofer, "Malpedia," 2021, https://malpedia.caad.fkie.fraunhofer.de/.

[56] P. Paganini, *Security Affairs*, https://securityaffairs.co/wordpress/category/apt, 2021.

[57] S. B. Rothman, "Understanding data quality through reliability: a comparison of data reliability assessment in three international relations datasets," *International Studies Review*, vol. 9, no. 3, pp. 437–456, 2007.

[58] K. Geers, D. Kindlund, N. Moran, and R. Rachwald, *WORLD WAR C: Understanding NationState Motives behind Today's Advanced Cyber Attacks*, 2013.

[59] K. H. Leetaru, *The GDELT Project*, https://www.gdeltproject.org/, 2021.

[60] T. World Bank, *World Development Indicators*, https://databank.worldbank.org/source/world-development-indicators, 2021.

[61] United Nations Statistics Division, *UNSD Data Bank*, https://data.un.org/, 2021.

[62] I. Monetary Fund, *World economic outlook databases*, https://www.imf.org/en/Publications/SPROLLs/world-economic-outlook-databases#sort=%40imfdate%20descending, 2021.

[63] T. Maurer, *Cyber Mercenaries: The State, Hackers, and Power*, Cambridge University Press, Washington, 2018.

[64] D. Denning, *How the Chinese Cyberthreat Has Evolved*, The Conversation, Melbourne, Australia, 2017.

[65] National Cyber Security Centre, *Reckless Campaign of Cyber Attacks by Russian Military Intelligence Service Exposed*, https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed, 2018.

[66] King Faisal Center for research and I. Studies, *Iran's Cyber-attacks Capabilities*, 2020.

[67] Parsons and M. George, *Understanding The Cyber Threat From Iran*, https://www.f-secure.com/en/consulting/our-thinking/understanding-the-cyber-threat-from-iran, April 2019.

[68] Public-Private Analytic Exchange Program, *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar*, 2019.

[69] M. Hjortdal, "China's use of cyber warfare: espionage meets strategic deterrence," *Journal of Strategic Security*, vol. 4, no. 2, pp. 1–24, 2011.

[70] J. R. Biden Jr, *Interim National Security Strategic Guidance*, Executive office of the president Washington D, Washington, DC, USA, 2021.

[71] R. Maness and B. Valeriano, *Russia's Coercive Diplomacy: Energy, Cyber, and Maritime Policy as New Sources of Power*, Springer, Berlin, 2015.

[72] J. Vijayan, *India's Cybercrime And APT Operations On the Rise. 23 September 2020*, https://www.darkreading.com/threat-intelligence/india-s-cybercrime-and-apt-operations-on-the-rise.

[73] The National Counterintelligence and Security Center, *Foreign Economic Espionage in Cyberspace*, 2018.

[74] ThaiCERT, *Threat group cards: a threat actor encyclopedia*, 2020.