Hacking Pattern in The EU Based On Core-Periphery Concept

Kerolos Ghaly and Tanusree Sengupta*
Christliches Jugenddorfwerk Deutschlands gemeinnütziger e. V. (CJD,)International School Braunschweig - Wolfsburg

Citation: Ghaly K. and Sengupta T. (2022) Hacking Pattern in the EU Based On Core-Periphery Concept, *International Journal of Interdisciplinary Research Methods*, Vol.9, No.3, pp.21-46

ABSTRACT : *Hacking and weak cyber-security affects many sectors. Nowadays, it is considered a part a political weapon. The study aims to test the existence of a hacking pattern within the 27 European countries (EU). Metadata collected from various reliable sources were tested and considered to identify the core-periphery pattern. Diverse statistical techniques were used to alleviate and spot the detected anomaly within the collected data. A new index was devised to smooth the effect of data anomaly and produce comparable data. Location Quotient (LQ) was also derived to compare to the publicly available cybersecurity indices (International Telecommunication Union; ITU) to the newly devised index from the current study. Investigating the existing pattern of hacking in EU seems to follow a core-periphery concept, which is mastered by factors like geopolitical position, internet users, and economic level. The current study might offer new frontiers to support cybersecurity in threatened countries.*

KEYWORDS:core-periphery concept, cyber-security, european union, gross domestic product, information and communications technology.

INTRODUCTION

Hacking is the unauthorized access to data digitally stored on a system or computer (Jaquet-Chiffelle and Loi, 2020). In the European countries (EU), as of 2019, 33% of the population have been victims of hacking attacks (Ergöçün, 2020).

Analysis of recent worldwide Cyber attacks displays that it is an active situation that requires a careful global spatial analysis to identify the connection among the locations of hacker's organizations and their targets. More specifically it is increasingly becoming a geopolitical weapon. Volker Kozok is a famous German lieutenant colonel in the armed forces. He had first investigated the security leaks after the Russian activity in the Crimea region of Ukraine (February and March 2014) that was repeated at the beginning of 2021 (Reuters, 2021). Kozok sees that cooperation between the cyber and geo-experts is key to security against the global threats caused by cyber attacks (Conklin, 2019). Noteworthy, this type of attack was intensified just before the start of the current war on 24 Feburary 2022. The European parliament brief (Przetacznik and Tarpova, 2022) has assessted the cybersecurity to Ukraine making use of the Eurpean cyber-sanctions authorities to protect its public, energy, financial and business sectors. A month after the war, CNN has broadcasting an urgent announcement by the American president Joe Biden to further strenghting the cyber defense covering business sectors (Vazquez et al., 2022). Thus, continous mapping of cyberattacks to localize the interdisciplinary hackers' activities is a geospatial approach that can relief the current limitations and support cybersecurity (Bowcut, 2021; Kumar, 2021).

This is sufficiently true for various sectors such as political, financial or health sectors. In 2017, the systemic risk barometer by Depository trust clearing company conducted a survey that ranked cyber risk on top (DTCC; Leibrock, 2017). Very, recently,the Financial Stability Board (FSB) has asserted that terms related to third-party risk like 'insider threat' should be considered. This term has emerged due to the increaisng dependency on third-party services and prolonged working remote during the pandemic time (FSB, 2022). In Germany, laws and regulations to secure a threat-resistant cyber are continuously considered by Banking and Security Trading Acts (Niethammer et al., 2022) and the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik; BaFin) have issued a comprehensive review on cybersecurity as a challenge for the public sector and the financial industry (BaFin, 2020). The defence is weaker in the developing countries; as the previous president of the United Nations, Lazarous Kapambwe, has described; "*The economic impact and consequences of cyberattacks against critical physical infrastructure, the banking system, national health systems, essential government and industry databanks and services could be extremely high*" Accordingly, the United Nations has continuously confirmed that developing countries are more targeted for cyber attack (United Nations news, 2011). These countries are likely to suffer from weak IT infrastructure, which would justify their vulnerability to cyber threats. These striking statistics and political directions were the motivation to investigate on this topic.

The current article examines the hacking patterns within the EU and investigates a comparative vulnerability of the selected countries. The three major objectives of this study are to investigate the relation of Gross Domestic Product (GDP) per capita and internet access with hacking patterns, the differences between western and eastern EU countries concerning the core-periphery concept, and the vulnerability of hacking represented by the identified patterns within the selected EU countries. At the end of investigation, the research question "*To what extent does the existing pattern of hacking in the EU confirm the existence of a core-periphery*?" will be answered.

LITERATURE/THEORETICAL UNDERPINNING

The current work is based on an extensive literature survey of the available resources on the topic including a preparatory analysis of statistics available on hacking using the previous expert articles such as that by the German expert Wolfgang Bock (Munich) and his colleagues in London (Bock et al., 2014).

To better understand a country´s vulnerability to hacking, the hacking vulnerability index has been devised by the authors. The hacking vulnerability index combines three of the most influential factors of hacking. These factors are GDP per capita, number of crypto-currency owners and the percentage of the populations with internet access. Countries were individually ranked as per their values in each factor. The sum of the three ranks divided by their numbers (i.e. 3) is taken as values for the newly devised hacking vulnerability index for each capita.

The concept of Immanuel Wallerstein´s core-periphery model (Goldfrank , 2000) has been borrowed to further adapt and analyse the hacking patterns within the selected east and west EU countries (Figure 1). The original model demonstrates that core countries are more economically developed and exploit periphery countries for resources and labour. Additionally, semi-periphery countries are described to stand in between the core and periphery hackers in terms of development.

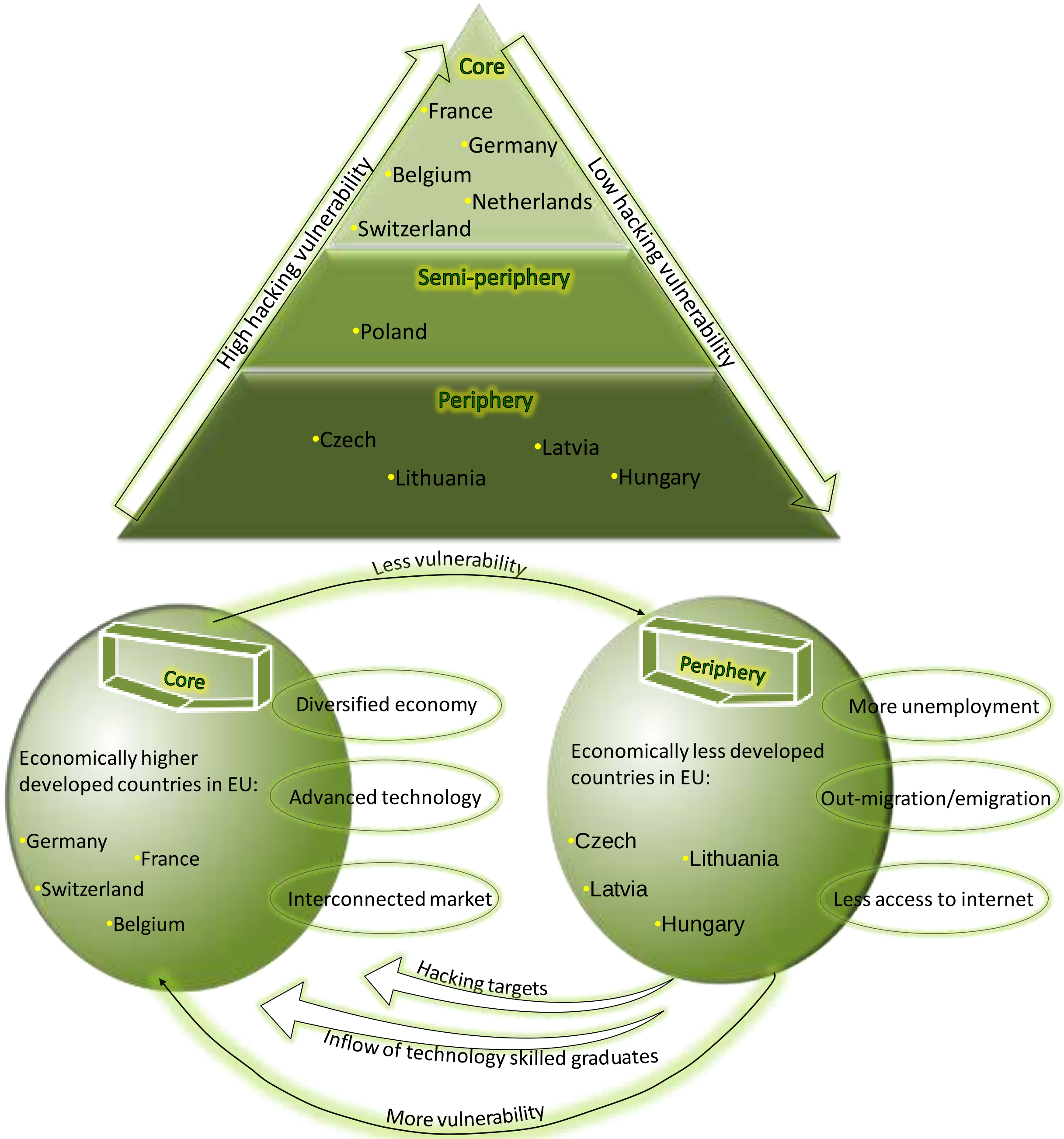


Figure 1. Adapted core-periphery concept from Immanuel Wallerstein (Goldfrank , 2000)

In order to adapt Wallerstein´s core-periphery model to fit the topic of the current study, core countries were set to be more vulnerable to hacking than the periphery countries. The reason for this is that core countries have a higher level of economic development, which means they have more advanced technology, a more connected firm market, and a diverse economy. All of which are attractive to hackers to target this group of countries. Meanwhile, in the periphery countries, there is more unemployment, less internet access, and higher emigration (Goldfrank , 2000). The most common destination for emigrants is the core countries, which welcome technologically qualified graduates. As a result, core countries are more vulnerable to hacking than peripheral countries. Major hacking techniques among these countries are displayed in Figure 2.

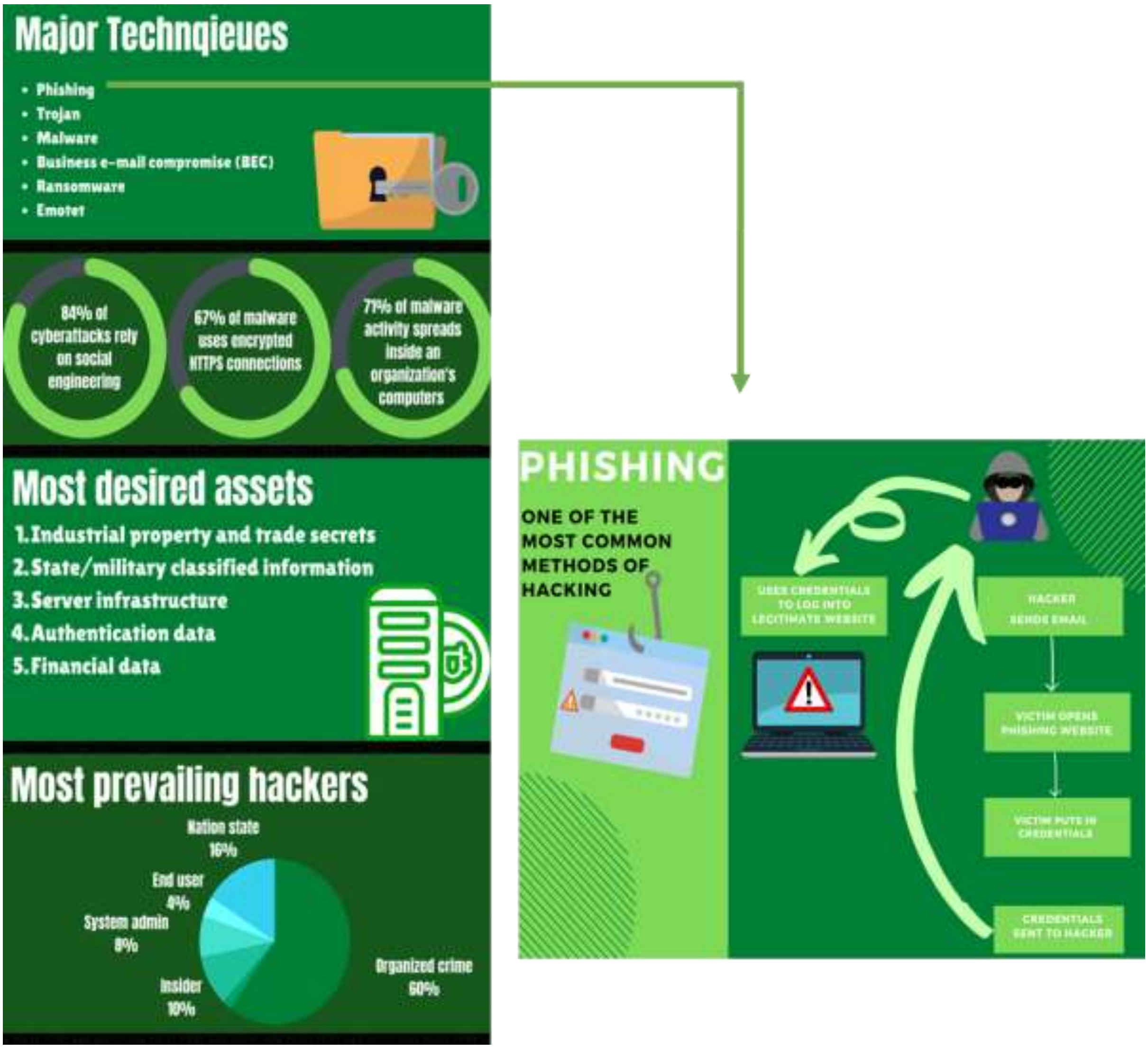

Major Technqieues
• Phishing
• Trojan
• Malware
• Business e-mail compromise (BEC)
• Ransomware
• Emotet
84% of cyberattacks rely on social engineering
67% of malware uses encrypted HTTPS connections
71% of malware activity spreads inside an organization's computers
Most desired assets
1. Industrial property and trade secrets
2. State/military classified information
3. Server infrastructure
4. Authentication data
5. Financial data
Most prevailing hackers
Nation state 16%
End user 4%
System admin 8%
Insider 10%
Organized crime 60%
PHISHING
ONE OF THE MOST COMMON METHODS OF HACKING
USES CREDENTIALS TO LOG INTO LEGITIMATE WEBSITE
HACKER SENDS EMAIL
VICTIM OPENS PHISHING WEBSITE
VICTIM PUTS IN CREDENTIALS
CREDENTIALS SENT TO HACKER

Figure 2. Major hacking techniques

Infographic made using Canva (https://www.canva.com/en_gb) with base information from ENISA (2019/2020)

METHODOLOGY

The number of people going online via mobile internet is continuously growing, which affects the total European internet users as well. The growth of the internet infrastructure can be well-translated to 530 million subscribed to mobile internet service in Western Europe alone, which is estimated as 1.33 subscriptions per person[3].

Technological competitiveness is a continuous battle. All the great innovations that are made possible with a larger amount of internet users in the EU also open the frontiers for hackers to use new analogous methods that facilitate them to gain access to sensitive data. A stepwise scheme including the literature and statistical methods of research has been created in Figure 3 to cover these aspects.

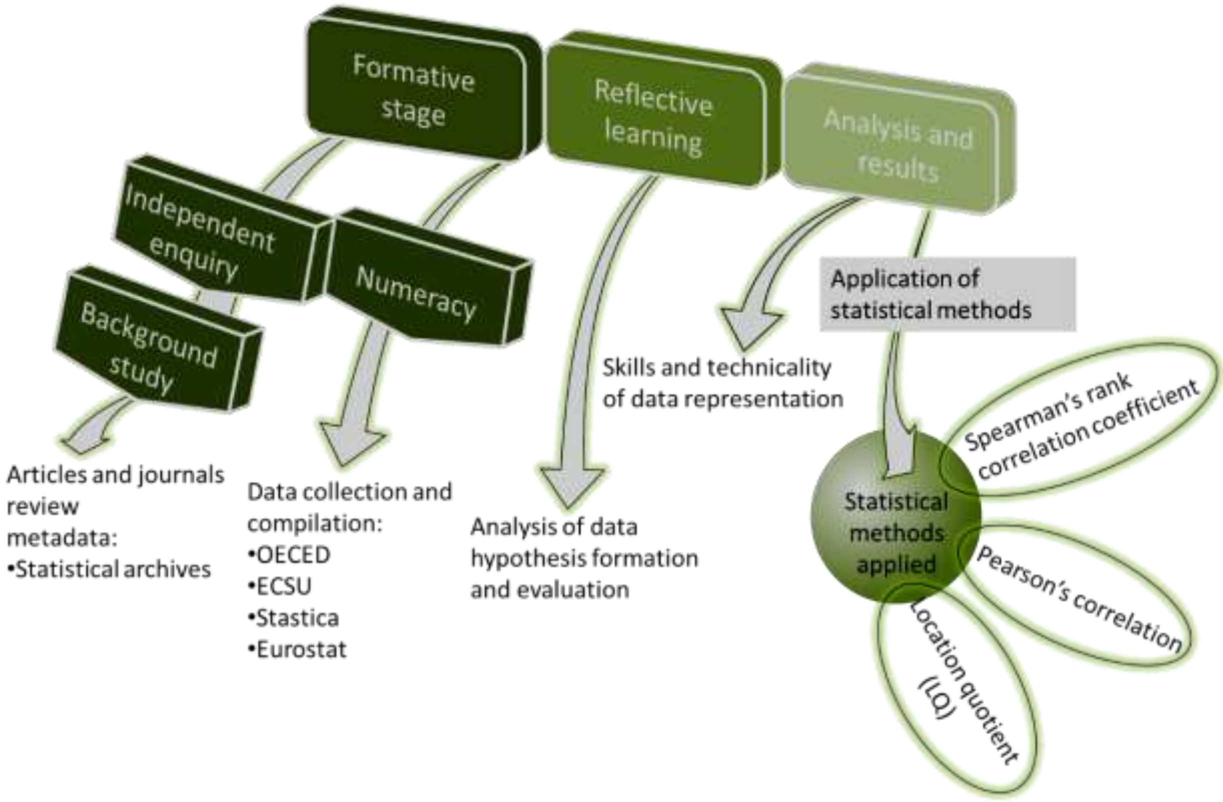

Formative stage
Reflective learning
Analysis and results
Independent enquiry
Numeracy
Background study
Application of statistical methods
Skills and technicality of data representation
Articles and journals review metadata:
•Statistical archives
Data collection and compilation:
•OECED
•ECSU
•Stastica
•Eurostat
Analysis of data hypothesis formation and evaluation
Statistical methods applied
Spearman's rank correlation coefficient
Pearson's correlation
Location quotient (LQ)

Figure 3. Plan for methodology of research

Hypotheses

Based on the theoretical background to study the research question two main hypotheses were derived:

Hypothesis 1: There is a divide between east and west EU countries in hacking pattern;

a. Western EU countries are more vulnerable to hacking than eastern EU countries.
b. GDP per capita is directly proportional to the number of machines hacked.

Hypothesis 2: Resilience to hacking differs among the EU members;

a. Core and periphery countries differ in cybersecurity measures in relation to hacking vulnerability.
b. More ICT graduates ensure a better resilience to hacking.

Selection of samples

Although the EU has 27 members, collecting complete EU data needs more access facilities and authorization. Nonetheless, based on the literature search, EU countries were sampled based on data accessibility. The political and historical configurations of the EU countries produce a significant economic divide between east and west EU members. Therefore, random stratified sampling has been used to select a total of 10 countries from the east and west EU. These 10 countries have been intentionally selected based on ensuring economic variability and allowing studying the diversified hacking patterns. This is presented in the following equations (*i-iii*) and Table 1, where x and $\bar{x}$ refer to the individual GDP per capita and the mean (average) value, respectively.

$$\bar{x} = \frac{\sum x}{n} \qquad i$$

$$\bar{x} = \frac{1281729.8}{27} \qquad \bar{x} = 47471.4$$

$\bar{x}$ = average GDP per capita

$\sum x$= summation of GDP per capita

n= total number of EU countries in 2021

Table 1. Deviation of GDP per capita from mean

EU members in 2021	GDP per capita, *x* (OECD, 2019)	*x*- $\bar{x}$=|*x*-47471.4|
Austria	58656.3	11184.863
Belgium	54918.1	7446.663
Bulgaria	24579.3	22892.137
Croatia	30231.2	17240.237
Cyprus	42861.3	4610.137
Czech Republic	43326.7	4144.737
Denmark	59870	12398.563
Estonia	38354.6	9116.837
Finland	51521.4	4049.963
France	49344.7	1873.263
Germany	56284.9	8813.463
Greece	30841.8	16629.637
Hungary	33961.6	13509.837
Ireland	89681	42209.563
Italy	44950.9	2520.537
Latvia	32013.3	15458.137
Lithuania	38805.8	8665.637
Luxembourg	119127.5	71656.063
Malta	48269.4	797.963
Netherlands	59674.8	12203.363
Poland	33858.3	13613.137
Portugal	36945	10526.437

Romania	32317	15154.437
Slovakia	32613.7	14857.737
Slovenia	41185	6286.437
Spain	42197.3	5274.137
Sweden	55337.9	7866.463

$$\text{Mean deviation of mean} = \frac{\sum|x-\bar{x}|}{n} \qquad ii$$

$$\text{Coefficient of mean deviation} = \frac{\text{Mean deviation of mean}}{\bar{x}} \qquad iii$$

$$\text{Coefficient of mean deviation} = \frac{13370.4}{47471.4}$$

$$\text{Coefficient of mean deviation} = 0.282$$

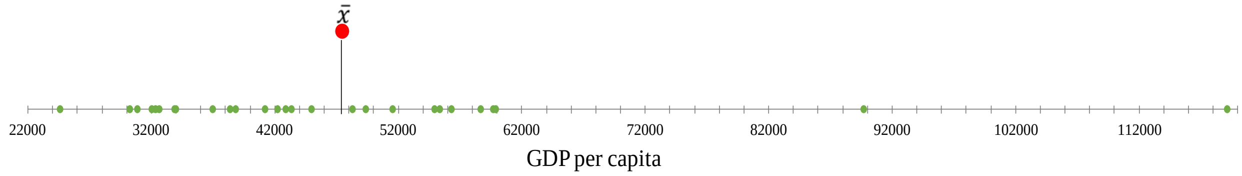


Figure 4. Deviation of GDP per capita from mean*

* $\bar{x}$ presents the mean. The 27 countries (●) depicted in Table 1, are ordered from the lowest to the highest GDP per capita.

Based on the displayed mean deviation in Figure 4 and dispersion analysis of the data, 10 countries were selected as representative EU members with east and west variability namely: Netherlands, Switzerland, Germany, France, Belgium, Czech, Poland, Hungary, Latvia, and Lithuania.

Statistical methods

The selection of the used statistical techniques passed through a screening followed by a pre-evaluation assessment. For example, the Mann-Whitney U test could not be applied in the current study due to its limitation as it is less significant compared to a parametric test. Other tests were initially taken into consideration but were declined during the study; such as the one-way ANOVA test. This test can be reliably applied using a single independent factor in combination with one dependent variable, which does not statistically fit the current data.

Pearson's correlation coefficient (equation *iv*) is a statistical test used to evaluate the statistical relationship, or association, between two continuous variables. It specifies the magnitude of the link or correlation as well as the direction of the relationship (https://www.statisticshowto.com/probability-and-statistics/correlation-coefficient-formula/).

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2)}} \qquad iv$$

r = Pearson correlation coefficient

n = number of samples

$\sum y \mid \sum x$ = sum of y or x

This statistical test has been used to compare data obtained from eastern and western EU countries. Since these two groups of countries are likely to have irregular distributions, the aforementioned pattern in Figure 4 was initially suggested. It assumes that there is a divide and the country is spotted in a separate deviated position.

Location quotients (LQ; equation *v*) are a type of statistic that is used in research to measure and evaluate the concentrations of different industries in a given region. They are important for determining the area's economic strengths and weaknesses. LQ was first adjusted to reflect the industrial portion of a region reflecting some economic data (i.e profits, GDP by metropolitan area, employment, etc.) and its share of the national total.

$$LQ = \left(\frac{x_1}{x}\right) \div \left(\frac{y_1}{y}\right) \qquad v$$

LQ= Location Quotient

$x_{1=}$ number in selected factor in the country

y_1= number in selected factor in the EU

x= total number in the country

y= total number in the EU

The LQ can be used in this studyas it allows the comparison of a single countries data compared to other EU countries. This is especially relevant when comparing aspects like a country's Information and Communications Technology (ICT) graduates to those in the EU. If the LQ is less than 1, the nation is under-represented in comparison to the rest EU, however, if it is equal to 1, the country is equally represented; and if it is greater than 1, the EU is over-represented (Christian, 2009).

$$\rho = 1 - \frac{6\sum d^2}{n(21)} \qquad vi$$

ρ = Spearman rank coefficient

$\sum d^2$ = sum of the squared difference between ranks

n = number of data points

The Spearman's rank-order correlation (ρ) is a nonparametric variant of the Pearson product-moment correlation. It determines the strength and direction of the monotonic relationship between the suggested two variables rather than the strength and direction of the linear relationship between these two variables, as Pearson's correlation does (Laerd statistics: https://statistics.laerd.com/statistical-guides/spearmans-rank-order-correlation-statistical-guide.php).

Accordingly, in this analysis, the Spearman rank is beneficial in determining the relationship between GDP per capita and hacking incidents because the two numbers are likely to differ significantly. As a result, Spearman's ranking correlation should be a far more accurate metric than Pearson's correlation coefficient.

RESULTS AND DISCUSSION

Adequate data could be surfed for a range of EU countries to study the questioned pattern. The availability of various online data sources does not mean they are all reliable. Accordingly, an effort was made to assure that each data source chosen for the current study is credible. After evaluating the available sources, either International Unions or verified International data banks were used. These sources include the International Telecommunication Union (ITU, 2020), Eurostat (2018) and the Organization for Economic Co-operation and Development (OECD, 2019). All data were assembled to figure two hypotheses in the current study.

Hypothesis 1

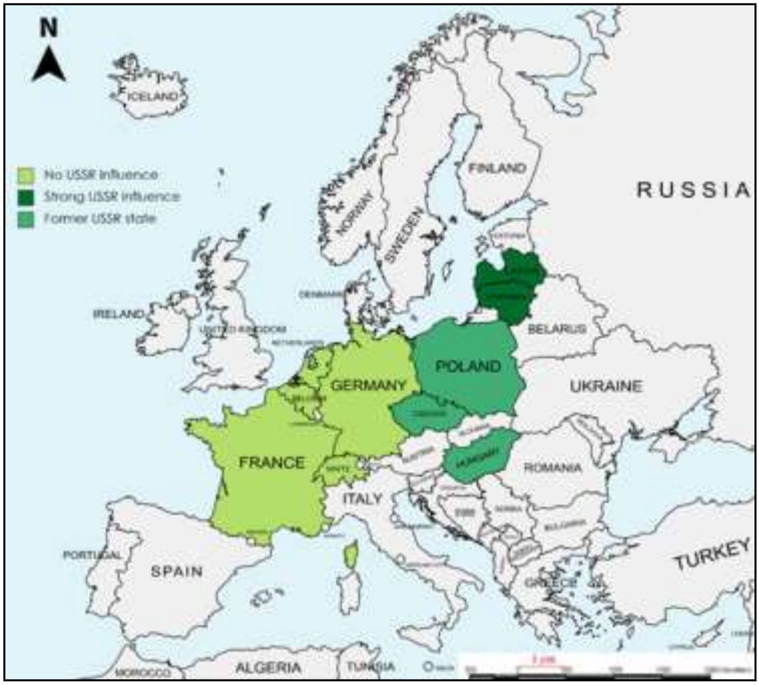
There is a divide between east and west EU countries in hacking pattern

a. Western EU countries are more vulnerable to hacking than Eastern EU countries

b. GDP per capita is directly proportional to the number of machines hacked

The influence of the Union of Soviet Socialist Republics (USSR) on the selected EU nations is one of the publicly indicated political historical consequences on the countries. Figure 5 ranks countries with no USSR influence to have the greatest GDP, followed by countries with a significant USSR impact and ends in former USSR countries. Nevertheless, countries with less USSR influence have both higher GDP per capita and more crypto-currency owners. Primarily, this shows a divide in economic power between east and west due to the historic effect of the USSR. However, the higher owner number of crypto-currency is more likely to attract hackers as it holds greater financial value to them than GDP per capita. This is because crypto-currency is expected to be an instant advantage by hackers. Meanwhile, getting financial value from GDP per capita is more complicated as GDP reflects the lively economic activity, which does not mean that an attractive monetary value is directly available.

A

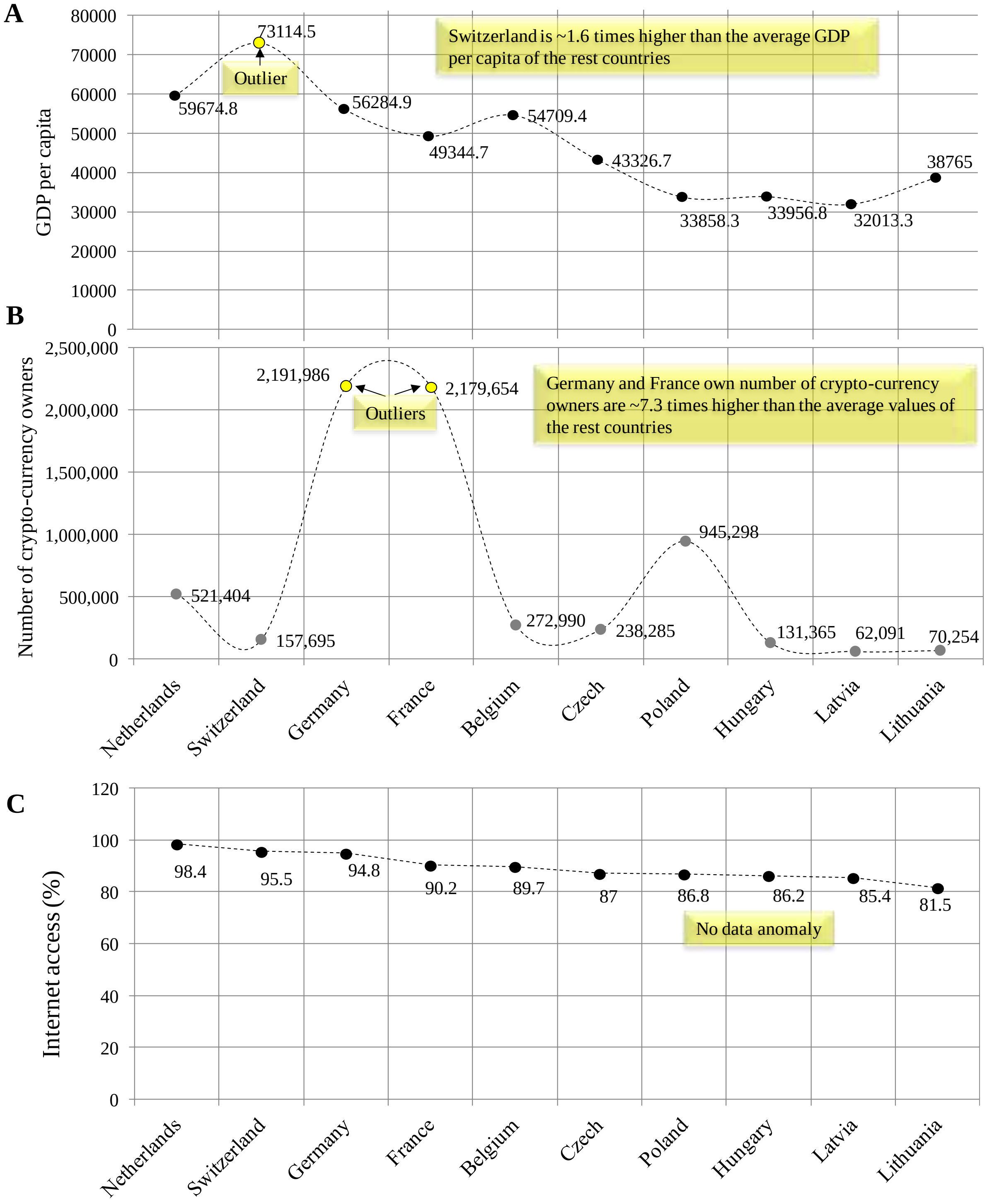


B

Country	GDP/capita (USD), 2019[1]	Number of crypto-currency owners, 2020[2]
Netherlands	59,674.8	521,404
Switzerland	73,114.5	157,795
Germany	56,284.9	2,191,986
France	49,344.7	2.179,654
Belgium	54,709.4	272,990
Czech	43,326.7	238,285
Poland	33,858.3	945,298
Hungary	33,956.8	131,365
Latvia	32,013.3	62,091
Lithuania	38,765.0	70,254

Figure 5. A) USSR influence on selected EU countries and B) GDP per capita.
Data sourced from:
[1]OECD iLibrary (2019) GDP and spending. Available at: https://doi.org/10.1787/4537dc58-en
[2]Triple A Cryptocurrency across the world (2020) Available at: https://triple-a.io/crypto-ownership/
Map was made using MapChart (https://mapchart.net/europe.html) and publicy available information from Britannica (Robert et al. accessed in October 2022)

Plotting GDP per capita (Figure 6A) and number of crypto-currency owners (Figure 6B) for each country indicates the lack of a common pattern within the selected group of countries. This can be mathematically explained by the presence of outliers that deviate from the mean of >50% of the samples. For example Switzerland is a clear anomaly when considering its GDP comparing to other countries. Data anomaly among number of crypto-currency owners (Figures 5B and 6B) is stronger than their counter-parts in GDP per capita. Excluding individual values for Germany and France, shows an average number of crypto-currency of 299,923 for the rest countries. Interestingly, the average crypto-currency of the rest countries shows 14% of that for Germany and France average. This huge deviation not only enhances the pattern anomaly in number of crypto-currency compared to GDP per capita, but also diminishes the possiblility of having the same rank for the countries' GDP or crypto-currency.



Switzerland is ~1.6 times higher than the average GDP per capita of the rest countries

Germany and France own number of crypto-currency owners are ~7.3 times higher than the average values of the rest countries

No data anomaly

Figure 6. Pattern anomaly of GDP per capita (A) and number of crypto-currency owners (B) compared to the stable pattern of % of internet access (C)

Hacking vulnerability index; devised by the authors:

Many factors can elect a country to be vulnerable to hacking. The hacking vulnerability index has been devised by the authors to understand the propensity of hacking among the representative EU countries. The most common reasons for hacking vulnerability is the financial prosperity within a country and the accessibility for hackers to gain access to these financial assets. To rationalize that, I have created a hacking vulnerability index, where two points should be considered: (i) the parameters used to calculate the hacking vulnerability of the selected EU countries, which are based on the clustering method, where the country ranking was investigated. Ordering countries that have internet accesses as per their GDP per capita, number of crypto-currency owners and the percentage of the population who have accesses to the internet can create a ranking number for each (Table 2). The average value of the obtained three rank numbers gives the hacking vulnerability indices that compile with the aforementioned most crucial factors. (ii) the second considerable point is the intended purpose of this index. The numerical values for GDP per capita (Figure 6A) and number of crypto-currency owners (Figure 6B) vary immensely even for a sole country. Moreover, a relatively stable pattern for the values presenting the % of internet access (Figure 6C) cannot compensate the huge deviation observed among the other two factors (Figures 6 and 7).

Accordingly, a single value summarizing the vulnerability of each country to hacking would alleviate this deviation. Ranking the countries within each factor is intended to merge the three factors for each country in a single index by calculating their mean. This index is presented for a smoother comparison (Figures 8 and 9).

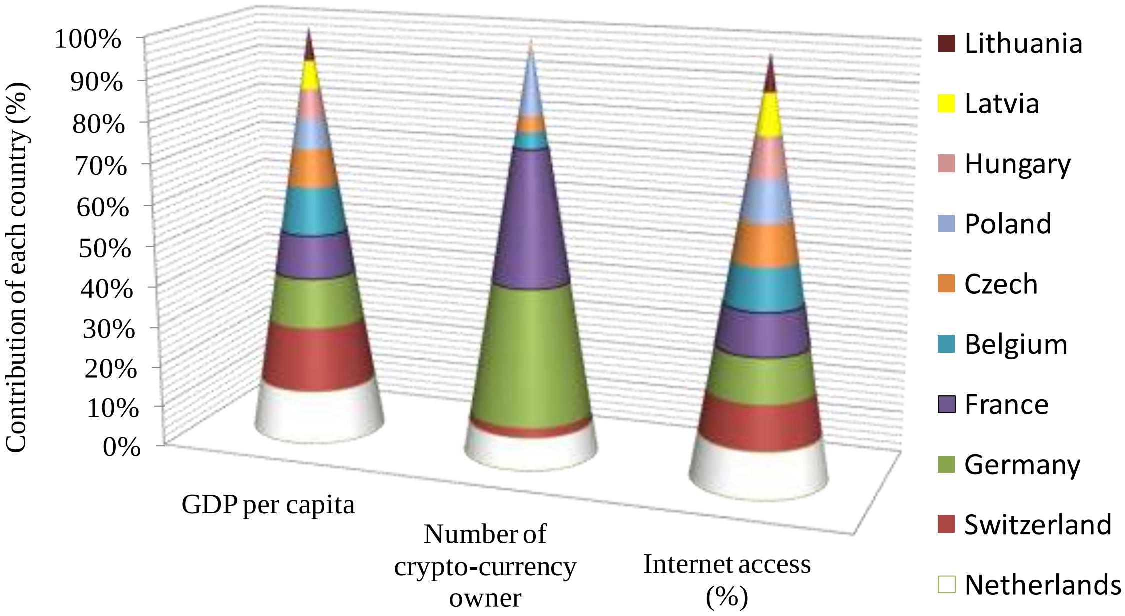


Figure 7. Percentage contribution of countries in the three factors used to devise the hacking vulnerability index

Table 2. Hacking vulnerability index devised by the authors

Country	GDP per capita (2019)[1]	GDP rank	Number of crypto-owners (2020)[2]	Crypto-rank	Internet access (%) (2019)[3]	Access rank	Rank average*
Netherlands	59674.8	9	521,404	7	98.4	10	8.6
Switzerland	73114.5	10	157,695	4	95.5	9	7.6
Germany	56284.9	8	2,191,986	10	94.8	8	8.6
France	49344.7	6	2,179,654	9	90.2	7	7.3
Belgium	54709.4	7	272,990	6	89.7	6	6.3
Czech	43326.7	5	238,285	5	87	5	5
Poland	33858.3	2	945,298	8	86.8	4	4.6
Hungary	33956.8	3	131,365	3	86.2	3	3
Latvia	32013.3	1	62,091	1	85.4	2	1.3
Lithuania	38765	4	70,254	2	81.5	1	2.3

*The average of the three ranks is termed the hacking vulnerability index.
Data were sourced from:
[1]OECD iLibrary (2019) GDP and spending. Available at: https://doi.org/10.1787/4537dc58-en
[2]Triple A Cryptocurrency across the world (2020) Available at: https://triple-a.io/crypto-ownership/
[3]OECD (data sourced from 2019) Information and communication technology (ICT) - Internet access - OECD Data. Available at: https://data.oecd.org/ict/internet-access.htm

A hacking vulnerability index close to 10 means the country is highly vulnerable to hacking, while indices closer to 0 indicate minor or no vulnerability to hacking. The countries that were found to be the most vulnerable to hacking were Netherlands and Germany, sharing a hacking vulnerability index of 8.6. Meanwhile, the country with the lowest vulnerability to hacking was Latvia with a hacking vulnerability index of 1.3.

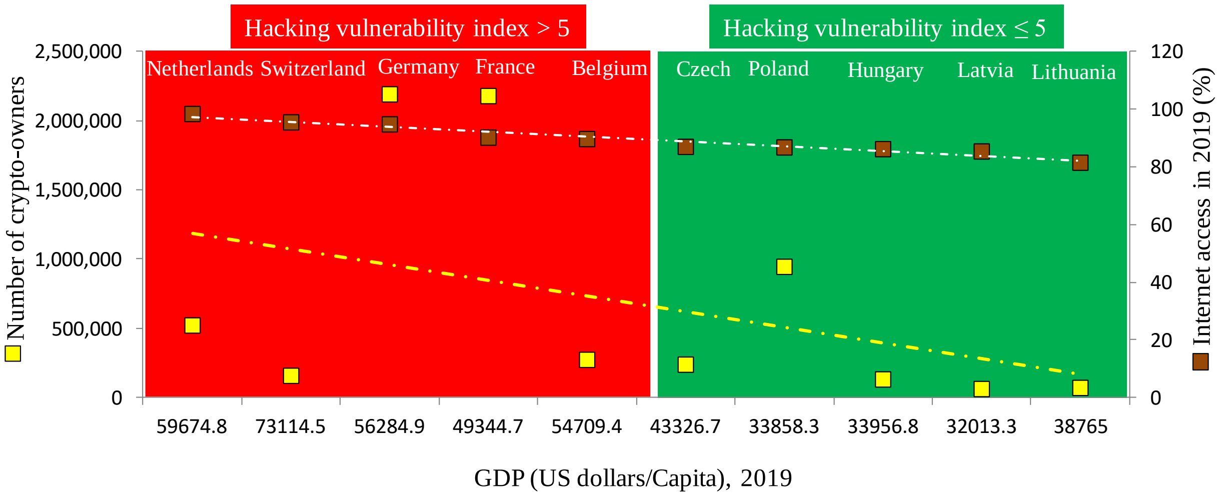


Figure 8. Hacking vulnerability graph

Plotting the numerical values of GDP per capita, percentage of the population with internet access and the number of crypto-currency owners in one graph (Figure 8) shows not only data deviation (two Y- and the lower X-axes in Figure 8) but also outliers (i.e yellow line of best fit). On the other hand, the individual values of hacking vulnerability indices (Table 2) grouped the countries into two groups (Figure 8); a group highlighted in red for indices more than 5 and in green for those equal or less than 5. The average values of the three factors used to set the hacking vulnerability index ± their standard deviation (SD), shows that the strong anomaly of number of crypto-currency owners (Figure 6B) agrees with the statsitically unaccepted SD that shows values close or higher than the mean (Table 3). Simultaneously, the hacking vulnerability index facilitates the use of a colour indicator to reflect the range of hacking vulnerability, which alleviates the high deviation among the original values and makes them more meaningful for interpretation.

Table 3. Average values of the three factors used to construct the hacking vulnerability index ± SD

Factor used to rank countries in hacking vulnerability index	Average values for countries with hacking vulnerability index >5	Standard deviation (±)	Average values for countries with hacking vulnerability index ≤5	Standard deviation (±)
1) GDP per capita	58625.66	8915.992	36384.02	4,616
2) Number of crypto-currency owners	1,064,746	1,031,810 🚫	289,459	373,324 🚫
3) Internet access (%)	93.72	3.700946	85.38	2.25655
Hacking Vulnerability index	**8**	**0.967988**	**3.24**	**1.553383**

🚫 Indicates SD values that are unacceptably close or even higher than the mean. Step-wise calculation is presented at Supplementary Table 1

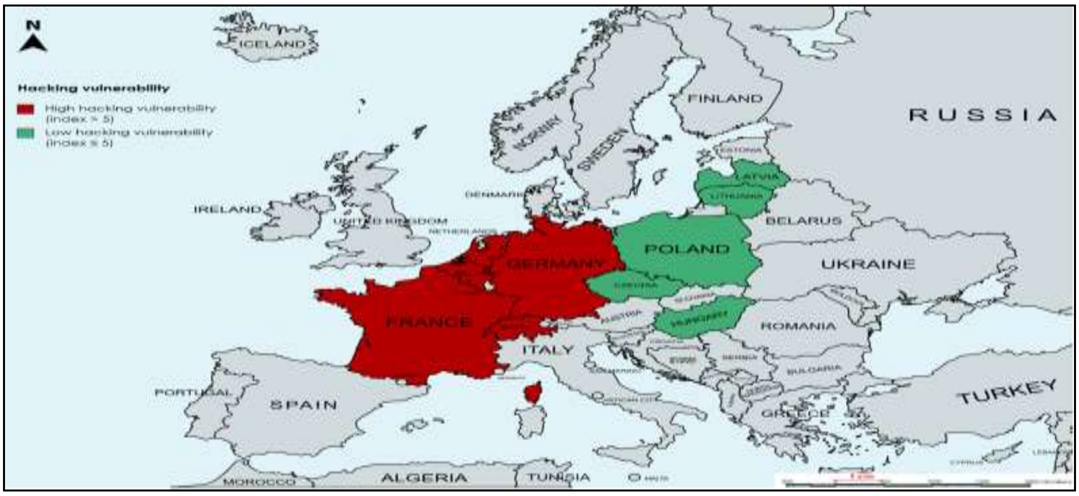


Figure 9. Mapping of hacking vulnerability index. Map was made using MapChart (https://mapchart.net/europe.html)

To our knowledge, considering the calculation of the hacking vulnerability index and graphing it with its factors has not been addressed before. Therefore it can be used to examine hypothesis 1 a. "*Western EU countries are more vulnerable to hacking than eastern EU countries*". To investigate this hypothesis, Figure 9 is useful as it maps and translates the hacking vulnerability index to a visible geographical factor. Interpreting Figure 8, shows that the hacking vulnerability distribution can be divided into two groups. It appears that western EU countries have a higher hacking vulnerability than the eastern EU countries under study. Therefore, hypothesis 1 (a) can be accepted as western EU countries are more vulnerable to hacking than eastern EU countries.

Table 4. Spearman: GDP per capita and percentage of systems hacked

Country	GDP per capita (X-value)[1]	Percentage of systems machines (Y- value)[2]	X_{rank}	Y_{rank}	d (X_{rank}- Y_{rank})	d^2
Netherlands	59674.8	17.64	2	1	1	1
Switzerland	73114.5	1.69	1	10	-9	81
Germany	56284.9	3.61	3	7	-4	16
France	49344.7	5.41	5	3	2	4
Belgium	54709.4	1.99	4	9	-5	25
Czech	43326.7	2.74	6	8	-2	4
Poland	33858.3	3.99	9	6	3	9
Hungary	33956.8	4.83	8	4	4	16
Latvia	32013.3	4.49	10	4	5	25
Lithuania	38765	6.40	7	2	5	25

Data were sourced from:
[1] OECD iLibrary (2019) GDP and spending. Available at: https://doi.org/10.1787/4537dc58-en
[2] Statista (data sourced from 2019) Cybercrime: Europe's most & least secure countries, from January to October 2019. Available at: https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/

$\rho = 1 - \frac{6\sum d^2}{n(n^2-1)}$ *vii* $\sum d^2 = 206$ $\rho = -0.249$

n = number of the selected EU member countries
x = GDP per capita
y = percentage of systems hacked
d = rank difference between the variables
$\sum d^2$= sum of the squared difference between the ranks

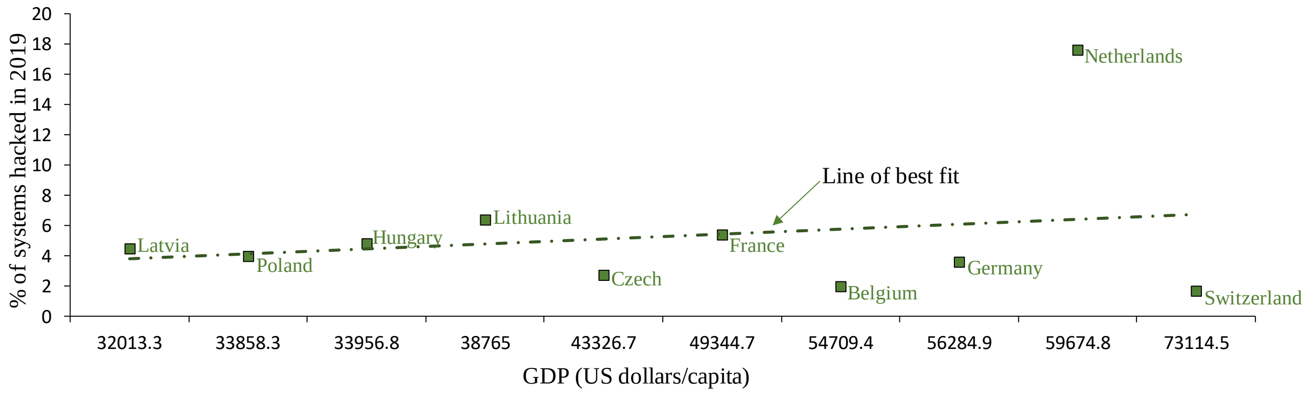
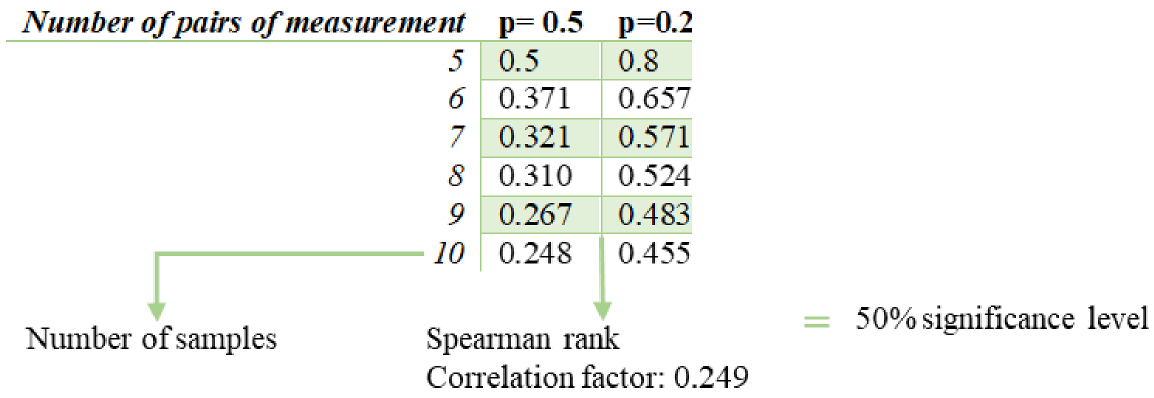


Figure 10. Scatterplot presenting possible effect of GDP per capita on percentage of systems hacked in 2019



Number of pairs of measurement	p= 0.5	p=0.2
5	0.5	0.8
6	0.371	0.657
7	0.321	0.571
8	0.310	0.524
9	0.267	0.483
10	0.248	0.455

Number of samples
Spearman rank
Correlation factor: 0.249
= 50% significance level

Figure 11. Significance level for Spearman analysis (Ramsey, 1989)

The calculations from Table 4 and Figure 10 indicate that there is a poor relationship between GDP per capita and the percentage of systems hacked, a very weak negative trend is identifiable. However, in this case, possible justification would be that high-income countries could have better cybersecurity infrastructure. Cybersecurity is further studied in hypothesis 2. Furthermore, Figure 11 (adapted from published data by Ramsey, 1989 illustrated at Supplementary Table 2) shows that the correlation must be disregarded because its significance shows that it is only 50% dependable. Figure 10 displays outliers, which are likely to be the main reason for the low

Spearman correlation. Nevertheless, it should be concluded that GDP per capita does not correlate with the number of a country hacking incidence. As a result, hypothesis 1 (b); "*GDP per capita is directly proportional to the number of machines hacked*" is disproved through Spearman correlation analyses confirm that GDP per capita is not directly proportional to the number of hacking.

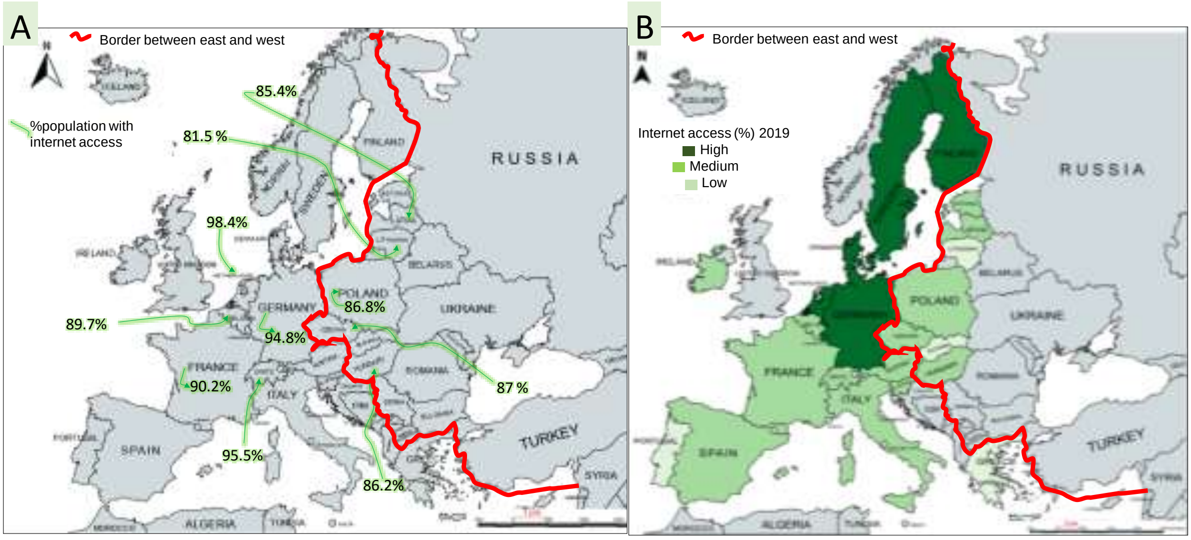


Figure 12. Mapping the percent of population with internet access in 2019
A) Mapping with the individual percentage for each country under study.
B) Pattern of internet accesses.

Maps were made using MapChart (https://mapchart.net/europe.html)

The representative countries have viable data as they follow the same pattern as the EU. Considering the research question, the east-west pattern displayed in Figure 12 confirms an identifiable divide between the EU countries based on internet access. The link between internet access and hacking cases has been previously confirmed in the aforementioned hacking vulnerability index. Figure 12A depicts a map that shows the percentage of the populations who have internet access as of 2019 for 5 western and 5 eastern EU countries. The amount of internet users is used as the key to analyzing the hacking pattern and the associated vulnerability (Figure 9). It is connoted that a higher amount of internet users is directly proportional to the number of possible victims for hackers to attack their systems. Noteworthy, a country with more internet users are expected to have a better-digitalized infrastructure than that with fewer internet users. This should also mean better cybersecurity and a well-alerted system of defence against hacking attacks. However, this may not always be the case as there may not be enough security measures in place.

Hypothesis 2

Resilience to hacking differs among the EU members

a. Core and periphery countries differ in cybersecurity measures in relation to hacking vulnerability
b. More ICT graduates ensure a better resilience to hacking

In Hypothesis 1, the 10 representative countries were grouped as per the various elements of the hacking vulnerability index into core and periphery groups (Table 5). The location quotient (LQ) was derived to be used as a comparative index between the hacking vulnerability index devised by the authors (hypothesis 1) and the cybersecurity index from the publicly available data (International Telecommunication Union, ITU, 2020). The LQ effectively compares the two groups of core or periphery with respect to the two indices serving as an applicable rationale for the 2nd hypothesis.

Table 5. Selected core and periphery countries

Core country	Periphery Country
Netherlands	Czech
Switzerland	Poland
Germany	Hungary
France	Latvia
Belgium	Lithuania

$$\boldsymbol{LQ} = \frac{(HVI\ \div \sum HVI)}{(CSI\ \div \sum CSI)} \qquad viii$$

LQ = Location quotient
HVI = Hacking vulnerability index (of either core or periphery country group)
$\sum HVI$ = summation of hacking vulnerability index for all 10 of the representative countries
CSI = Cybersecurity index for the 10 representative countries
$\sum CSI$ = Summation of cybersecurity index for whole EU

Core countries:

$$\boldsymbol{LQ_C} = \frac{(38.4 \div 54.6)}{(929.4 \div 2464.6)}$$

$\boldsymbol{LQ_C} = 1.87$

Periphery countries:

$$\boldsymbol{LQ_p} = \frac{(16.2 \div 54.6)}{(929.4 \div 2464.6)}$$

$\boldsymbol{LQ_p} = 0.79$

As indicated under subsection 2C of this essay (Statistical methodology), the value calculated for LQ (equation *viii*) can be below 1, which indicates underrepresentation in the region of the core or periphery group, while 1 means it is equally presented and a value above 1 means that it overrepresentation in the region. As the LQ value for core countries (LQ_C = 1.87) is above 1, the core countries have more cybersecurity than hacking vulnerability. Meanwhile, the periphery countries have a value below 1 (LQ_p = 0.79) indicating that cybersecurity is underrepresented in relation to their hacking vulnerability. Not only does this confirm the core-periphery division, but it also demonstrates that core countries have better cybersecurity compared to their vulnerability. In light of the LQ findings, it has been determined that periphery countries appear to have insufficient cybersecurity for their hacking vulnerability, while core countries face the opposite. Thus, hypothesis 2 (a) is confirmed as the LQ values identify that core countries differ from periphery countries in cybersecurity measures with relation to their hacking vulnerability.Information and communication technologies graduates are presumed to be more resilient to hacking due to their studies. Thus, a country with more ICT graduates would be expected to have fewer cases of hacking. Figure 13 presents the percentage of graduates in different fields of study to give an overview of the distribution of graduation within the EU**.**

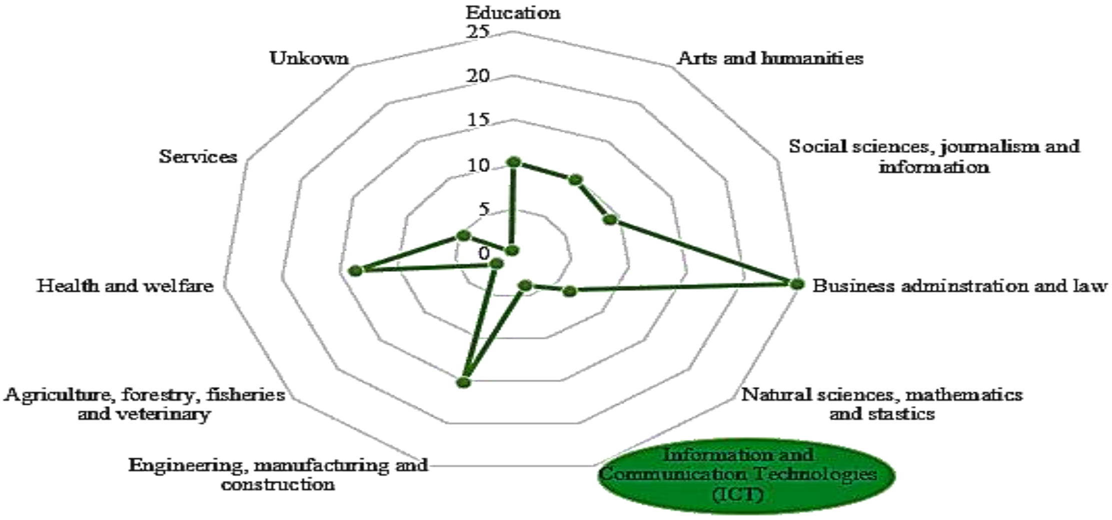


Figure 13. Percentage of graduate distribution in the EU (Eurostat, 2018)

Table 6. Pearson´s correlation: machines hacked and ICT graduates

Countries	Percentage of machines hacked in EU, 2019 (x)[a]	Percent ICT graduates, 2018 (y)[b]	xy	x^2	y^2
Netherlands	17.64	2.8	49.392	311.1696	7.84
Switzerland	1.69	2.5	4.225	2.8561	6.25
Germany	3.61	4.9	17.689	13.0321	24.01
France	5.41	3.5	18.935	29.2681	12.25
Belgium	1.99	2.1	4.179	3.9601	4.41
Czech	2.74	4.9	13.426	7.5076	24.01
Poland	3.99	3.8	15.162	15.9201	14.44
Hungary	4.83	4.6	22.218	23.3289	21.16
Latvia	4.49	4.7	21.103	20.1601	22.09
Lithuania	6.4	3.1	19.84	40.96	9.61
∑	52.79	36.9	186.169	468.163	146.07

Data were sourced from:
[a]Statista (data sourced from 2019) Cybercrime: Europe's most & least secure countries, from January to October 2019. Available at: https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/

[b] Eurostat (2018) Tertiary education statistics. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Tertiary_education_statistics#Graduates

$$r = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2)}}$$

$$r = \frac{10 \times 186.17 - 52.79x36.9}{\sqrt{(10 \times 468.16} - 2786.78)(10 \times 146.07 - 1361.61}$$

$$r = -0.199$$

The Pearson correlation coefficient, calculated in Table 6 and the work below it, shows a weak negative correlation. This indicates that more ICT graduates do not necessarily mean there is a lower number of machines hacked. This result disproves the statement (hypothesis 2 b) that more ICT graduates in a country ensure a better resilience to hacking.

IMPLICATION TO RESEARCH AND PRACTICE

This article has focused to study the hacking pattern within selected EU countries. Correlation to their geopolitical position and economic level was a focus. Different from EU, data reflecting a clear hacking pattern from the developing countries are scarce. Thus, the current study might offer frontiers opportunities to find possible measures supporting these threatened countries.

CONCLUSION

The research question *"To what extent does the existing pattern of hacking in the EU confirm the existence of a core-periphery?"* was the main prompt for thisarticle. It was investigated using a systemic research approach incorporating an intensive literature survey of the available academic sources like published reports, journals, books and exploration of the metadata sources like Statista, and OECD data, followed by hypotheses formation and statistical testing of the collected variables to reach a valid conclusion.

Hypothesis 1: *´There is a divide between east and west EU countries in hacking pattern*` had two sub-hypotheses. To explore the first sub-hypothesis 1 a; *´Western EU countries are more vulnerable to hacking than eastern EU countries,* the hacking vulnerability index I devised the, which incorporates GDP per capita, the number of crypto-currency owners and the percentage of the population with internet access, into one comparable value for each county. Further, the spearman analysis and mapping were used to test the hypothesis. Accordingly, western EU countries were found to be more vulnerable to hacking than eastern EU countries. In the second sub- hypothesis 1 b; *´GDP per capita is directly proportional to the number of machines hacked*` Spearman and scatterplot have confirmed that GDP per capita is not directly proportional to the number of machines hacked.

Hypothesis 2: *´Resilience to hacking differs among the EU members*` was divided into two sub-hypotheses. The first sub-hypothesis 2 a; *´Core and periphery countries differ in cybersecurity measures in relation to hacking vulnerability*` prompted the use of location quotient, which was applied to this sub-hypothesis proving it as valid. In the second sub-hypothesis, 2 b; *´More ICT graduates ensure a better resilience to hacking*` Pearson correlation analysis was used, which disproved the hypothesis.
Overall the core-periphery is displayed in the existing pattern of showing the division in hacking vulnerability through resilience differences. This was also seen by the comparative analysis of cybersecurity and hacking vulnerability. However, the pattern is only confirmed when taking multiple factors into account such as the newly devised hacking vulnerability index. Oppositely, when two factors such as GDP per capita and the number of hacking cases are taken into account, no clear pattern could be confirmed. The core-periphery model that was originally proposed by Immanuel Wallerstein (1971) has been extended and modified to make it relevant to the present context. The model has not been applied directly, but the core-periphery concept has been borrowed in the process of geographical pattern identification.

FUTURE RESEARCH

The challenge of studying the complex topic of hacking prompted us to devise the hacking vulnerability index, which with its compiled data factors allows a thorough study of the hacking vulnerability patterns.

Theoretically, it would have been more rigorous if this study was expanded through personal interaction to collect primary data from the countries where no data were publicly available. Further, this study should be expanded in the future to study the core-periphery hacking patterns within different non-EU areas to be used as a comparison to the EU.

While there is a limitation of available secondary data, it was still possible to conduct the current study using the public EU sites and related articles. Additionally, the results of this study prompt future investigation on the topic to give a global understandable scale, which could benefit further developments in the cybersecurity and resilience industries.

References

BaFin perspectives Issue 1 (2020) *Cyber security: a challenge for the public sector and the financial industry*.https://www.bafin.de/SharedDocs/Downloads/DE/BaFinPerspektiven/2020/bp_20-1_

Ben Conklin (2019) *Cybersecurity: The Geospatial Edge*, *German Cybersecurity Experts Use GIS to Uncover Patterns of Attacks.* ESRI Blog. https://www.esri.com/about/newsroom/blog/german-cybersecurity-experts-use-gis/

Bock, W. Field, D. Zwillenberg, P. and Rogers, K. (2014) *The Mobile Internet Economy in Europe*. The connected world, Boston Consulting Group (bcg). https://www.bcg.com/publications/2014/telecommunications-technology-digital-mobile-internet-economy-europe

Bowcut, S. (2021) *Cybersecurity in the financial services industry*. Cybersecurity guide. https://cybersecurityguide.org/industries/financial/

Christian, D. (2009) Essential Geographical Skills. Oxford University Press. ISBN: 9781408503331. https://www.google.de/books/edition/Essential_Geographical_Skills/EhlrPgAACAAJ?hl=de

ENISA, Threat Landscape report (2019/2020) *European Union Agency for cybersecurity: Main incidents in the EU and worldwide*. Edited by Marco Barros Lourenço and Louis Marinos, pp 1-26. ISBN: 978-92-9204-354-4, DOI: 10.2824/552242. DOI: 10.2824/552242

Ergöçün, G. (2020) *EU: 33% of citizens hit by cyberattacks in 2019*. Economy, Europe. https://www.aa.com.tr/en/economy/eu-33-of-citizens-hit-by-cyberattacks-in-2019/1730868

Eurostat (2018) Tertiary education statistics. Available at: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Tertiary_education_statistics#Graduates

FSB (2022) *Achieving greater convergence in cyber incident reporting–Consultative document.* https://www.fsb.org/2022/10/achieving-greater-convergence-in-cyber-incident-reporting-consultative-document/

Goldfrank, W., L. (2000) *Paragidm Regained? The Rules of Wallerstein's World-System Method.* Journal of World-Systems Research 6, 150–195. https://doi.org/10.5195/jwsr.2000.223

International Telecommunication Union (ITU), *Global Cybersecurity Index 2020.* https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Jaquet-Chiffelle, D.-O. and Loi, M. (2020) *Ethical and Unethical Hacking*. In: Christen, M., Gordijn, B., Loi M. (eds) The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, 21. pp 179-204. Springer, Cham. https://doi.org/10.1007/978-3-030-29053-5_9

Kumar, V. (2020). *Cybersecurity latest news*: *Powering the role of cybersecurity with geospatial data.* https://www.analyticsinsight.net/powering-the-role-of-cybersecurity-with-geospatial-data/

Leibrock, M. (2017) DTCC connection. https://www.dtcc.com/dtcc-connection/articles/2017/june/20/dtccs-leibrock-discusses-q1-2017-systemic-risk-barometer-survey-results

Niethammer, A., Rieks, D., Herfurth, C., Saerbeck S. (2022) *Cybersecurity laws and regulations Germany2022*. https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/german

OECD (data sourced from 2019) Information and communication technology (ICT) - Internet access-OECD Data. https://data.oecd.org/ict/internet-access.htm

OECD iLibrary (2019) GDP and spending. https://doi.org/10.1787/4537dc58-en

Przetacznik, J. and Tarpova, S. (2022) Russia's war on Ukraine: Timeline of cyber-attacks (PE 733.549-June 2022). EPRS | European Parliamentary Research Service. www.europarl.europa.eu/thinktank

Ramsey, P.H. (1989) *Critical values for Spearman's rank order correlation*. Journal of educational statistics 14, 245-253. https://journals.sagepub.com/doi/10.3102/10769986014003245

Reuters (22. February 2021) *Ukraine accuses Russian networks of new massive cyber attacks.* https://www.reuters.com/article/us-ukraine-cyber-idUSKBN2AM1VF

Robert, C., Dewdney, J.C., Pipes, R.E., McCauley, M. "*Soviet Union*". *Encyclopedia Britannica*, https://www.britannica.com/place/Soviet-Union. Accessed 20 October 2022

Statista (data sourced from 2019) Cybercrime: Europe's most & least secure countries, from January to October 2019. Available at: https://www.statista.com/chart/20914/share-of-european-computers-that-experienced-cyberattacks/

Triple A Cryptocurrency across the world (2020) Available at: https://triple-a.io/crypto-ownership/

United Nations news, *Developing countries most vulnerable to cyberattacks-UN* (2011) https://news.un.org/en/story/2011/12/397922

Vazquez, M., Judd, D., Lyngaas, S. and Cohen, Z., (March 2022) *Biden warns business leaders to prepare for Russian cyber attacks,* CNN Politics. https://edition.cnn.com/2022/03/21/politics/biden-russia-cyber-activity/index.htm

Supplementary data

Supplementary Table 1. Step-wise calculation of the standard deviation (SD) presented in Table 3 within the main article.

Color code is based on grouping the countries as per the hacking vulnerability indices (red for values >5, green for values ≤5)

Used formula to calculate the SD is: $\sqrt{\frac{\sum(x-\bar{x})^2}{(n-1)}}$

Country	GDP per capita (x$_1$)	x-$\bar{x}_1$	(x-$\bar{x}_1$)^2	Σ(x-$\bar{x}_1$)^2	n-1	(Σ(x-$\bar{x}_1$)^2)/4	SD
Netherlands	59674.8	1049.14	1100694.74	317979648	4	79494912	8915.991919
Switzerland	73114.5	14488.84	209926485				
Germany	56284.9	-2340.76	5479157.38				
France	49344.7	-9280.96	86136218.5				
Belgium	54709.4	-3916.26	15337092.4				
$\bar{x}_1$	58625.66						

Country	GDP per capita (x$_1$)	x-$\bar{x}$	(x-$\bar{x}_1$)^2	Σ(x-$\bar{x}_1$)^2	n-1	(Σ(x-$\bar{x}_1$)^2)/4	SD
Czech	43326.7	6942.68	48200805.6	85243723.1	4	21310931	4616.376369
Poland	33858.3	-2525.72	6379261.52				
Hungary	33956.8	-2427.22	5891396.93				
Latvia	32013.3	-4370.72	19103193.3				
Lithunia	38765	2380.98	5669065.76				
$\bar{x}_1$	36384.02						

Country	Number of crypto-currency owners (x$_2$)	x-$\bar{x}_2$	(x-$\bar{x}_2$)^2	Σ(x-$\bar{x}_2$)^2	n-1	(Σ(x-$\bar{x}_2$)^2)/4	SD
Netherlands	521,404	-543,342	2.9522E+11	4.25853E+12	4	1.06463E+12	1031810.239
Switzerland	157,695	-907,051	8.22741E+11				
Germany	2,191,986	1,127,240	1.27067E+12				
France	2,179,654	1,114,908	1.24302E+12				
Belgium	272,990	-791,756	6.26877E+11				
$\bar{x}_2$	1064745.8						

Country	Number of crypto-currency owners (x$_2$)	x-$\bar{x}_2$	(x-$\bar{x}_2$)^2	Σ(x-$\bar{x}_2$)^2	n-1	(Σ(x-$\bar{x}_2$)^2)/4	SD

Czech	238,285	-51,174	2618737337	5.57484E+11	4	1.39371E+11	373324.3645
Poland	945,298	655,839	4.30125E+11				
Hungary	131,365	-158,094	24993586361				
Latvia	62,091	-227,368	51696025530				
Lithunia	70,254	-219,205	48050656661				

Supplementary Table 1 (continued)

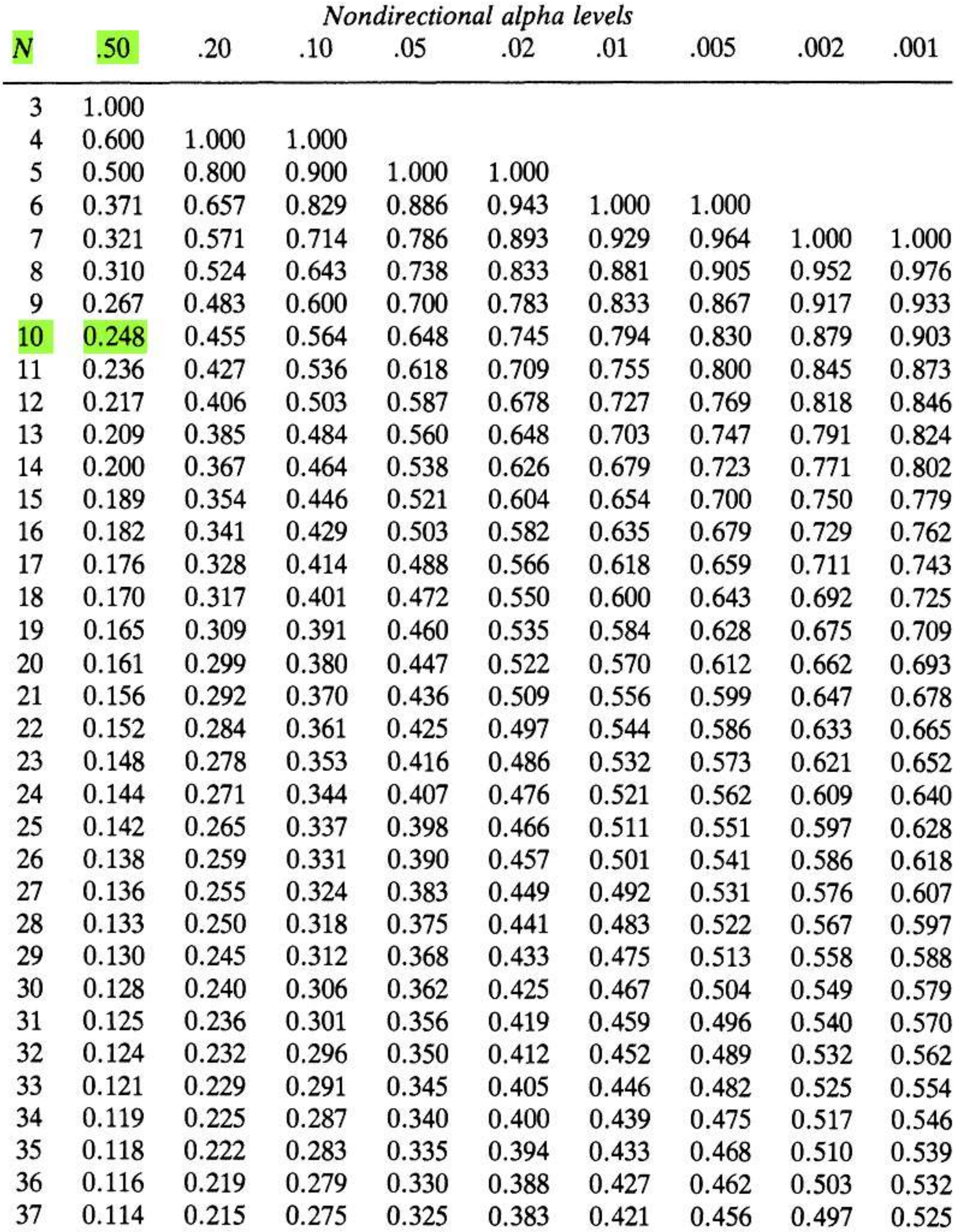
Country	Internet access (%, x_3)	$x-\bar{x}_3$	$(x-\bar{x}_3)^2$	$\Sigma(x-\bar{x}_3)^2$	n-1	$(\Sigma(x-\bar{x}_3)^2)/4$	SD
Netherlands	98	5	21.9024	54.788	4	13.697	3.700945825
Switzerland	96	2	3.1684				
Germany	95	1	1.1664				
France	90	-4	12.3904				
Belgium	90	-4	16.1604				
$\bar{x}_3$	93.72						

Country	Internet access (%, x_3)	$x-\bar{x}_3$	$(x-\bar{x}_3)^2$	$\Sigma(x-\bar{x}_3)^2$	n-1	$(\Sigma(x-\bar{x}_3)^2)/4$	SD
Czech	87	1.62	2.6244	20.368	4	5.092	2.256546033
Poland	87	1.42	2.0164				
Hungary	86	0.82	0.6724				
Latvia	85	0.02	0.0004				
Lithunia	82	-3.88	15.0544				
$\bar{x}_3$	85.38						
$\bar{x}_2$	289458.6						

Country	Hacking vulnerability index (X)	$x-\bar{x}$	$(x-\bar{x})^2$	$\Sigma(x-\bar{x})^2$	n-1	$(\Sigma(x-\bar{x})^2)/4$	SD
Netherlands	9	1	0.8464	3.748	4	0.937	0.967987603
Switzerland	8	0	0.0064				
Germany	9	1	0.8464				
France	7	0	0.1444				
Belgium	6	-1	1.9044				
$\bar{x}$	7.68						

Country	Hacking vulnerability index (X)	$x-\bar{x}$	$(x-\bar{x})^2$	$\Sigma(x-\bar{x})^2$	n-1	$(\Sigma(x-\bar{x})^2)/4$	SD
Czech	5	2	3.0976	9.6520	4	2.413	1.553383404
Poland	5	1	1.8496				
Hungary	3	0	0.0576				
Latvia	1	-2	3.7636				
Lithunia	2	-1	0.8836				
$\bar{x}$	3.24						

Supplementary Table 2. Identification of significance level for Spearmann rank coefficient of 0.249 and sample size n=10



	Nondirectional alpha levels								
N	.50	.20	.10	.05	.02	.01	.005	.002	.001
3	1.000								
4	0.600	1.000	1.000						
5	0.500	0.800	0.900	1.000	1.000				
6	0.371	0.657	0.829	0.886	0.943	1.000	1.000		
7	0.321	0.571	0.714	0.786	0.893	0.929	0.964	1.000	1.000
8	0.310	0.524	0.643	0.738	0.833	0.881	0.905	0.952	0.976
9	0.267	0.483	0.600	0.700	0.783	0.833	0.867	0.917	0.933
10	0.248	0.455	0.564	0.648	0.745	0.794	0.830	0.879	0.903
11	0.236	0.427	0.536	0.618	0.709	0.755	0.800	0.845	0.873
12	0.217	0.406	0.503	0.587	0.678	0.727	0.769	0.818	0.846
13	0.209	0.385	0.484	0.560	0.648	0.703	0.747	0.791	0.824
14	0.200	0.367	0.464	0.538	0.626	0.679	0.723	0.771	0.802
15	0.189	0.354	0.446	0.521	0.604	0.654	0.700	0.750	0.779
16	0.182	0.341	0.429	0.503	0.582	0.635	0.679	0.729	0.762
17	0.176	0.328	0.414	0.488	0.566	0.618	0.659	0.711	0.743
18	0.170	0.317	0.401	0.472	0.550	0.600	0.643	0.692	0.725
19	0.165	0.309	0.391	0.460	0.535	0.584	0.628	0.675	0.709
20	0.161	0.299	0.380	0.447	0.522	0.570	0.612	0.662	0.693
21	0.156	0.292	0.370	0.436	0.509	0.556	0.599	0.647	0.678
22	0.152	0.284	0.361	0.425	0.497	0.544	0.586	0.633	0.665
23	0.148	0.278	0.353	0.416	0.486	0.532	0.573	0.621	0.652
24	0.144	0.271	0.344	0.407	0.476	0.521	0.562	0.609	0.640
25	0.142	0.265	0.337	0.398	0.466	0.511	0.551	0.597	0.628
26	0.138	0.259	0.331	0.390	0.457	0.501	0.541	0.586	0.618
27	0.136	0.255	0.324	0.383	0.449	0.492	0.531	0.576	0.607
28	0.133	0.250	0.318	0.375	0.441	0.483	0.522	0.567	0.597
29	0.130	0.245	0.312	0.368	0.433	0.475	0.513	0.558	0.588
30	0.128	0.240	0.306	0.362	0.425	0.467	0.504	0.549	0.579
31	0.125	0.236	0.301	0.356	0.419	0.459	0.496	0.540	0.570
32	0.124	0.232	0.296	0.350	0.412	0.452	0.489	0.532	0.562
33	0.121	0.229	0.291	0.345	0.405	0.446	0.482	0.525	0.554
34	0.119	0.225	0.287	0.340	0.400	0.439	0.475	0.517	0.546
35	0.118	0.222	0.283	0.335	0.394	0.433	0.468	0.510	0.539
36	0.116	0.219	0.279	0.330	0.388	0.427	0.462	0.503	0.532
37	0.114	0.215	0.275	0.325	0.383	0.421	0.456	0.497	0.525

The Table is a screenshot from
Ramsey, P.H. (1989) *Critical values for Spearman's rank order correlation*. Journal of educational statistics 14, 245-253. https://journals.sagepub.com/doi/10.3102/10769986014003245