Hindawi
Human Behavior and Emerging Technologies
Volume 2022, Article ID 1230344, 12 pages
https://doi.org/10.1155/2022/1230344

Research Article

Investigating Installers of Security Software in 20 Countries: Individual- and Country-Level Differences

David Smahel, Lenka Dedkova, Lydia Kraus, Vaclav Matyas, and Vlasta Stavova

Faculty of Informatics, Masaryk University, Brno 60200, Czech Republic

Correspondence should be addressed to David Smahel; davsmahel@gmail.com

Received 23 March 2022; Accepted 7 May 2022; Published 1 June 2022

Academic Editor: Zheng Yan

This article provides detailed evidence about the installers of online security software on personal computers according to differences among clusters of countries and various other country characteristics. The study presents unique data based on real installations around the world. The data are based on a large-scale quantitative study ($N = 18{,}727$) which was prepared in cooperation with an international security company. The cluster analyses revealed four distinct clusters of software installers: those who install the software for a different user, those who are IT technicians and mostly install the software for other users, those who install the software for themselves and others on a shared computer, and those who install the software only for themselves. A second cluster analysis revealed four different country clusters. Within these clusters, countries handle online security software installation similarly; however, there are differences for the clusters according to industrialized, English-speaking countries and the cluster of developing countries. This study presents unique cluster analyses of the countries to shed light on the cross-culture differences in security software adoption and installation. The results implicate that software companies should consider providing different versions of the security software to match the country characteristics.

1. Introduction

The secure management of computers often starts with the installation of adequate online security software, such as antivirus software (in the remainder of this work, we define online security software as software that provides, at least, antivirus protection. The software may, however, offer additional features). Studies that have assessed online security software usage suggest that it is a prevalent security practice among end users. For instance, Ion et al. [1] found that it was the top self-reported security practice by end users. Similarly, in a census-representative survey among United States users, Redmiles et al. [2] found that 84% of the users reported using antivirus software.

Yet, in the second half of 2012, 40% of the computers in Egypt, 24% in South Africa, and 30% in India did not use antivirus software [3]. As of 2015, 24% of Windows OS computers worldwide were without antivirus software [4]. That means that many computers are potentially vulnerable to threats. For instance, research by Meisner [3] indicates that a computer without antivirus software is 5.5 times more likely to be exploited. Further research also indicates a negative correlation between antivirus software use and infection rates [5].

As online security software is installed (or enabled) by humans, it is necessary to understand who actually installs it so that future computer security awareness campaigns and educational interventions can be tailored more effectively to further increase computer protection rates. Knowledge about the installers of the software is also useful for software companies so that they can adapt their security to both the installers and the users. Until now, there have been only a limited number of studies about security software installers, and none of these studies used large-scale data from real software installations around the world. There is also a limited amount of studies on older adults and the aging population; the majority of studies used samples of students and/or youths. Our study fills this gap with a large-scale quantitative study of software installers ($N = 18{,}727$, 70% males, $M_{age} = 43.2$, $SD = 18.1$) from 20

countries who completed a short questionnaire at the end of the installation process of the home version of online security software from our industry partner, ESET, a major online security software provider. This data provides a new and unique understanding about the practice of security software installation.

Our study examines the installer's relationship to the computer (i.e., whether they are a user of the computer, the computer owner, or an IT professional) because previous studies show that end users may delegate the security of their own devices to other actors, such as Internet providers, IT technicians, friends, or family members [6–8]. Our study introduces an innovative cluster analysis to show who the installers of the security software are and how they differ from the users of the computers. This is also the first study to explore the differences among security software installers across countries. These results could be valuable for both the software companies and the policy makers to prepare effective educational strategies to establish proper security habits [9].

2. Theoretical Background

Our study is based on different research areas which we will introduce next.

2.1. Software Installation and Security Technology Adoption. The users and their role in the software installation process have primarily been studied in the context of smartphones, mainly due to the privacy-related decisions that users had to make in this context (e.g., the literature on Android app permissions; [10]). However, the literature about the installers of security software on desktop computers is scarce. Examples that are loosely related to our research are the works of Good et al. [11] and [12] which address End-User License Agreement (EULA) notices during the installation process of diverse software programs. However, while Good et al. [11] and [12] focus on the subsequent implications for the user-friendly design of such notices, our focus is to identify the different groups of security software installers.

We consider installation to be the moment at which a person decides to adopt a piece of software, so our work is also related to the research on the adoption of new technologies and, specifically, on the adoption of security features. Technology adoption research has traditionally used theoretical models, such as the technology acceptance model (TAM; [13]), the theory of planned behavior (TPB; [14]), and the innovation diffusion theory (IDT; [15]) to predict technology adoption. Regarding the adoption of security measures, TPB and protection motivation theory (PMT; [16]) have been applied most prominently in home computer security studies [17].

However, the use of these models, in general, and in the context of home computer security, in particular, has two limitations. First, these kinds of models rely on the assumption that the intention to use a technology is closely related to the actual adoption of that technology [18]. Second, traditional technology acceptance models seem to be insufficiently applicable in the context of security technology adoption [19] because the motivation to use security technologies differs from the motivation to use other consumer technologies. Furthermore, people who install the security software often differ from those who use and adopt the technology, as we show below.

2.2. Who Is Responsible for Computer and Device Security? Our work is based on the assumption that the software installer is not necessarily the user because studies on security and privacy management behavior show that many issues related to keeping ICT secure are often delegated to someone besides the primary device user or owner [6–8]. In general, users seem to turn to people they know for seeking security advice or technical help, such as friends or coworkers [2, 20, 21], but also to service providers and IT technicians [6, 20].

But who are the stakeholders actually involved in securing a computer? In a qualitative study of 20 households with children that focused on the household members' privacy and security decisions and the configuration and programming of technologies, Rode [22] distinguishes three types of households. First is a household where one person emerges as the "security czar" who is responsible for the digital safety of the other household members. A similar role was identified in other research; for instance, Kiesler et al. [23] mention a technical "guru" who may be or may not be a family member. This could be, for example, a tech-savvy teenager in the home who uses the Internet the most [23]. Also, Grinter et al. [24] found that, typically, the person who is the most technically knowledgeable in the family becomes the guru and helps other family members with ICT issues.

The second type of household in Rode's [22] study are self-support households, where the adults are each responsible for their own devices. Rode notes that the adults' technical knowledge is evenly distributed and perceived as high, so no one stands out as a security czar or the go-to person.

Finally, the third type is a household that seeks external help. It is labeled as an outside-support provider household. This includes those who do not have a person perceived as highly digitally skilled. In such cases, a common approach for the members of these households is to turn to the extended family, friends, or IT experts for assistance.

Contrary to Rode [22], Nthala and Flechais [6] do not distinguish between the types of households, but rather between the stakeholders who are responsible for the data security decisions made in the home environment. They identify two kinds of stakeholders: informal and business stakeholders. Whereas informal stakeholders include both people in the household and family, friends, and neighbors from outside the household, business stakeholders include Internet service providers, antivirus vendors, and organizations that perform awareness campaigns.

It is important to note that there is no consensus in the literature as to whether the home computer user should be considered an individual or part of the household: while the computer security studies described above take into account the household environment and the social context,

other studies consider the home user to be an individual who keeps their device secure (cf., e.g., [25]). Our study, which is based on real data from software installations, helps to clarify this issue.

The up-to-date studies of the installers of software used rather small samples, and they did not identify possible clusters of software installers. Our exploratory study tries to fill this gap, and therefore, we have the following research questions:

(1) Who are the installers of the security software? How are the clusters of the installers of security software determined, based on their demographics, their relationship to the computer, their level of computer skills, their perception of computers, and the objective system data of their computers (i.e., CPU, RAM, and OS version)?

(2) What are the clusters of countries, based on the variability of the clusters of the security software installers, the OS version, and the CPU size of the installers, and the following country-level indicators: network readiness, education, software piracy, Internet penetration, and GDP per capita?

3. Materials and Methods

In our study, we cooperated with an online security company, ESET, and collected large-scale data from the real installations of its security software around the world during five months (see below). We asked the software installers (i.e., the people who actually performed the installation) at the end of online security software installation about their relationship to the computer (i.e., whether they were the owners and whether they were the users of the computer). For users, we distinguished between sole users and users who shared the computer with others. We were further interested to cross-check whether the installation of online security software was a task for which people sought professional help. Subsequently, we asked whether the software installer was an IT technician. Lastly, we were interested in how the characteristics of software installers differed between countries. We used cluster analysis to find distinct groups of software installers under the assumption that the resulting clusters would correspond to the knowledge drawn from previous studies. Our cluster analysis is of an explorative nature; thus, we will discuss the commonalities and deviations in installation behavior as compared to the related work in Discussion of this article.

3.1. Procedure. The study was conducted in cooperation with ESET, an online security software company with more than 100 million users in more than 200 countries and territories (https://www.eset.com/int/about/). We received data from the users who installed the English version of the online security software solutions (specifically ESET Internet Security, ESET NOD32 Antivirus, ESET Smart Security, and ESET Smart Security Premium) between October 2016 and February 2017.

The original dataset obtained from ESET included data from 799,450 end-user installations (i.e., cases). To clean the dataset, we first excluded the cases with ESET's internal IP address ($N = 275$). Furthermore, in an attempt to remove multiple installations from the same computing device, we deleted the duplicate entries that were identified by combining hardware features, IP addresses, and hashed MAC addresses ($N = 50{,}380$), thereby removing approximately 6% of the entries from the original dataset. The cleaned dataset included 748,795 installations from 222 countries and territories. ESET put no restrictions on downloading the software to particular continents or countries. The geographic data showed that most installations (80.7% of the data) came from 20 countries. We focus on these 20 countries in our study.

The software installers were invited to complete a short questionnaire at the end of the installation process. After confirming their intention to fill out the questionnaire by clicking the link presented on the last screen of the installation process, the software installers were directed to a questionnaire hosted on the ESET webpages. The questionnaire was at least partially filled in by 4.2% of the software installers from 174 countries ($N = 31{,}447$). For our analyses, we selected those software installers who completed all of the crucial variables from the 20 most represented countries. The final analyzed sample consisted of 18,727 software installers, who represented 3.6% of the installations from the cleaned dataset.

Since the questionnaires were obtained only from a small portion of users, we compared the data available for all (i.e., hardware and software features) to check whether we would find substantial differences between users who did and did not complete the questionnaire. The differences were statistically significant, yet very small, mostly less than 2 percentage points. The negligible effect sizes (ranging from $\text{Phi} = 0.012$ to 0.030) confirm that the statistical significance ($p < 0.001$), in this case, is a consequence of the large sample size rather than of meaningful differences [26].

3.2. Measures. The data collected in the study are twofold: first, the data was obtained through the aforementioned self-reported questionnaire, which captured the software installers' basic demographics and a few additional characteristics. Second, ESET provided system data about each installation, which captured basic software and hardware features. Apart from the data collected in the study, we also used selected variables on the country level from external sources in order to interpret the country clusters. For instance, we used several country indicators, such as GDP, education, ICT penetration, and software piracy rate, because the related literature on malware infection rates, which is closely connected to the use of online security software, points to associations with these indicators [5, 27–29]. Since the data from ESET in our study were collected at the end of 2016 and at the beginning of 2017, we used the data from 2016 for country indicators, where possible.

The data obtained from questionnaires includes the following:

(1) Demographics. Users were asked to report their age, gender, and education (i.e., primary, secondary, and tertiary)

(2) The relationship to the computer of the person who installed the software. Software installers were asked "Regarding this computer, are you..." with multiple choice options: the owner, the sole user, one of multiple users, and IT technician. The data were further recategorized to reflect the ownership of the computer (0 = no, 1 = yes), the usage of the computer (1 = is not an actual user of the computer, 2 = is a sole user of the computer, and 3 = is one of the users of shared computer), and whether the person who installed the software was an IT technician (0 = no, 1 = yes)

(3) Computer skills. Software installers were asked whether they considered themselves to be skilled computer users on a 6-point scale ranging from (1) not at all skilled to (6) extremely skilled

(4) The perception of computers as un/safe devices. Software installers were asked whether they considered a computer to be, in general, safe against online attacks, such as by viruses or hackers. The answers ranged from (1) not at all safe to (6) absolutely safe

The system data from the installations includes the following:

(1) CPU performance. We used the PassMark CPU Mark criterion (https://www.cpubenchmark.net/) to categorize CPU performance into low-end, mid-low, mid-high, and high-end

(2) RAM size. This was recoded into four categories: 0-2 GB, 2-4 GB, 4-8 GB, and 8+ GB

(3) OS version. ESET provides solutions for the Windows operating system. Windows XP and Vista were represented only marginally ($N = 199$), so we omitted these cases from the analysis and used only Windows 7, Windows 8, and Windows 10

(4) Countries, identified from IP addresses by GeoIP2 (https://www.maxmind.com/en/geoip2-databases). The 20 countries included in this study are Australia, Bangladesh, Canada, Egypt, India, Indonesia, Islamic Republic of Iran, Israel, New Zealand, Pakistan, the Philippines, Romania, Saudi Arabia, Serbia, South Africa, Sri Lanka, Thailand, the United Arab Emirates, the United Kingdom, and the United States

The country-level indicators that we used for the interpretation of the clusters include the following:

(1) Gross domestic product (GDP) per capita. We used the data released by the World Bank [30]. GDP per capita shows the value of the country's goods and services converted to US dollars, divided by the country's population

(2) The network readiness index (NRI) by the World Economic Forum [31] is a composite index made up of 53 individual indicators distributed across different pillars. It uses data from external agencies, such as the World Bank and UNESCO, and their own surveys. The overall NRI reflects the countries' preparedness to reap the benefits of digital transformation. It ranges from 1 to 7, with 1 representing the lowest and 7 the highest readiness. We use the overall NRI and 4 other indicators from the WEF's dataset

(3) Software piracy rate describes unlicensed software units as a percentage of the total software units installed. This includes operating systems, business applications, and consumer applications, such as games, personal finance, and reference software [31]

(4) Tertiary education enrollment rate is the ratio of total enrollment, regardless of age, to the population of the age group that officially corresponds to the respective education level [31]

(5) Percentage of individuals using the Internet refers to the proportion of individuals who used the Internet in the preceding 12 months [31]

(6) Percentage of households with Internet access at home is the share of households with Internet access at home. It is calculated by dividing the number of in-scope households (where at least one household member is aged 15–74) with Internet access by the total number of in-scope households [31]

3.3. Analytical Strategy. The present study uses two cluster analyses: the first is to identify clusters of software installers and the second is to identify the clusters of countries. Cluster analysis is an explorative technique to identify groups of cases that are similar to each other in specified input variables [32]. We then describe the similarities within and the differences between the clusters, based on the variables that we obtained from the study and external sources.

3.4. Software Installer Clusters. First, we aimed to cluster the users involved in our study to better present the groups of software installers that actually install the online security software. Since we were specifically interested in the characteristics relevant to the usage of computers, we used four input variables: (1) the usage (i.e., whether the person installing the software was the sole user of the computer, one of the users of a shared computer, or a nonuser); (2) whether the person installing the software was an IT technician; (3) the users' computer skills; and (4) the extent to which the user perceives the computer as a safe device (see Measures). Since the first two variables are categorical and the other two are scales, we used two-step clustering. This method allows for the combining of these types of variables, and it is suitable for large datasets (Sarstedt and Mooi, [33]). The number of clusters in the solution was decided based on the Bayes Information Criterion (BIC) and the content evaluation of several clustering solutions. To ensure the stability

of the solution, we randomly split the sample into halves and ran the analysis on each half separately to see whether the two analyses would lead to similar clusters. Based on these procedures, the four-cluster solution was evaluated as stable and interpretable. The silhouette measure of cohesion and separation showed this to be a fair solution (value of 0.3). We then analyzed the differences among the four clusters, using other variables (i.e., system data and questionnaire data) in the study. We used chi-square tests with the Tukey post hoc test for categorical data and analysis of variance for scale data.

3.5. Country Clusters. The aim of the second cluster analysis was to identify similarities in software installer groups in different countries. To do this, we used the proportion of software installers' clusters from the previous analysis as input variables. We used a hierarchical cluster analysis with a median linkage method and squared Euclidean distance. The final number of clusters (i.e., four) was based on observing the distances among the clusters in the dendrogram and again on the clusters' interpretability. To ensure the stability of this cluster analysis solution, we used *K*-means clustering on the same data. Both methods' solutions corresponded to each other well, distinguishing similar clusters of countries and showing the stability of the four-cluster solution.

4. Results

Who are the installers of the security software? On average, the software installers in our study tended to be male (70.3%) and rather well-educated (78.8% tertiary education). Interestingly, the age range was wide: software installers were between 18 and 80 years old ($M = 43.24$, SD = 18.06).

As is apparent from the descriptive statistics (cf. Table 1), most of the people who installed the software were the computer owners (72%). This was expected, since we focused on the home edition of the product. Interestingly, this did not mean that they also used the computer: 47.0% of all installers reported that they are not the actual user of the computer. Of the 53% of installers who reported to use the computer, only 28.9% were the sole users of the computer, while 24.1% reported to be one of the users of a shared computer.

When it comes to computer skills and safety perceptions, the software installers reported above average skills ($M = 4.07$, SD = 1.40) on a 6-point scale and a medium level for perceiving computers to be, in general, safe devices against online attacks, such as by viruses or hackers, again on a 6-point scale ($M = 3.55$, SD = 1.79). A rather small group of all installers were IT technicians (6.9%).

Most installers used computers with mid-high (43.2%) or high-end (27.9%) CPU performance. RAM size fell mostly into the categories 2-4 GB (41.10%) or 4-8 GB (30.2%). Although many installers used the current operating system (Windows 10: 47.6%), the majority still used older operating systems (Windows 7: 41.4%; Windows 8: 11.0%).

Table 1: Software installers' usage and ownership of the computer.

Usage	Nonuser	User		Total
		Sole user	Sharer	
PC owner	42.8%	19.9%	9.4%	72.2%
Nonowner	4.1%	9.0%	14.7%	27.8%
Total	47.0%	28.9%	24.1%	100%

4.1. Software Installer Clusters. The first cluster analysis divided the sample into four groups of software installers. The relationship to and the usage of the computer were the most influential separating variables, so we used these variables to label the clusters (cf. Table 2).

Cluster 1: owner, but not a user. The first cluster (43% of the sample) consists of installers who are computer owners, but who do not use the computer personally. People in this cluster ($N = 8{,}025$) are mostly male (72.5%) and on average 40 years old ($M = 40.62$, Md. = 36.00; SD = 17.64). They self-identify as rather skilled computer users ($M = 4.17$; Md. = 4.00; SD = 1.45) and perceived computers as rather safe devices ($M = 3.98$; Md. = 4.00; SD = 1.86).

Cluster 2: IT technicians. The second cluster (7% of the sample) consists of all installers who reported being IT technicians ($N = 1{,}285$). Out of these, most of them (60%) were also not the actual user of the computer, though more than half of them own the computer (55.7%). Almost all respondents in this cluster were male (87.9%), and they represent the youngest clusters ($M = 35.23$, Md. = 36.00; SD = 17.64). Installers in this cluster consider themselves as having high computer skills ($M = 4.5$; Md. = 5.00; SD = 1.62), and it has the largest proportion of people with tertiary education (86%). They do not have a strong opinion regarding the safety of computers and perceive them, on average, as neither safe nor unsafe devices ($M = 3.36$; Md. = 3.00; SD = 1.88).

Cluster 3: users who share a computer. The third cluster (23% of the sample) consists of all installers who use the computer on a shared basis. All people in this cluster share the computer with someone else, though most of them are also computer owners (62%). Again, installers in this cluster are mostly male (71.1%) and on average 44 years old (i.e., older than the users in clusters 1 and 2) ($M = 44.01$, Md. = 44.00; SD = 17.92). They consider themselves to be moderately skilled ($M = 3.82$; Md. = 4.00; SD = 1.34). As in cluster 2, they do not have a strong opinion regarding the safety of computers and perceive them, on average, as neither safe nor unsafe ($M = 3.32$; Md. = 3.00; SD = 1.69).

Cluster 4: sole users. The fourth cluster (27% of the sample) is composed of all installers ($N = 5{,}105$) who are the sole users of the computer onto which they installed the software. Interestingly, only one-third of them own the computer (32.4%). This is the cluster with the largest proportion of females (32.8%), albeit they still represent a minority. With an average age of almost 49, people in this cluster represent the oldest installer group ($M = 48.69$, Md. = 52.00; SD = 18.02). Although they consider themselves to be rather skilled computer users ($M = 4.00$; Md. = 4.00; SD = 1.24), they consider the PC to be rather unsafe, which makes them

Table 2: Software installers' cluster overview.

Software installers' clusters		1	2	3	4	Difference tests
N		8025	1285	4312	5105	
%		42.85	6.86	23.03	27.26	
System data (%)						
RAM size	0-2 GB	17.60	16.10	15.50	7.80	$X^2(9) = 547.559$, $p < 0.001$, Cramer's $V = 0.099$
	2-4 GB	42.70	35.70	41.60	36.00	
	4-8 GB	30.40	30.30	33.10	39.40	
	More than 8 GB	9.20	17.90	9.80	16.80	
CPU	Low	5.50	2.90	4.60	3.40	$X^2(9) = 233.163$, $p < 0.001$, Cramer's $V = 0.067$
	Low-mid	26.50	21.00	25.00	19.50	
	High-mid	46.10	44.70	46.00	45.20	
	High	21.90	31.40	24.40	31.90	
OS version	Win7	36.40	33.90	36.90	27.30	$X^2(6) = 330.537$, $p < 0.001$, Cramer's $V = 0.094$
	Win8	15.30	14.00	12.60	9.10	
	Win10	48.30	52.10	50.50	63.60	
Questionnaire data, categorical (%)						
Gender	Male	72.50	87.90	71.10	67.20	$X^2(3) = 218.08$, $p < 0.001$, Cramer's $V = 0.11$
Education	Primary	3.20	2.50	2.20	1.50	$X^2(6) = 72.78$, $p < 0.001$, Cramer's $V = 0.060$
	Secondary	18.00	11.50	17.90	17.80	
	Tertiary	78.80	86.00	79.90	80.70	
Computer usage	Is not user	100.00	59.80	0.00	0.00	$X^2(6) = 35264.965$, $p < 0001$, Cramer's $V = 0.97$
	Sole user	0.00	24.00	0.00	100.00	
	One of the users	0.00	16.10	100.00	0.00	
Computer owner	Yes	97.90	55.70	62.00	32.40	$X^2(3) = 5699.683$, $p < 0.001$, Cramer's $V = 0.552$
IT technician	Yes	0.00	100.00	0.00	0.00	$X^2(3) = 18727.0$, $p < 0.001$, Cramer's $V = 1$
Questionnaire data, scales						
Age	*M*	40.62	35.30	44.01	48.69	$F(3, 18723) = 311.67$, $p < 0.001$, $\text{eta}^2 = 0.05$
	SD	17.64	14.83	17.92	18.02	
Computer skills	*M*	4.17	4.51	3.82	4.00	$F(3, 18723) = 109.26$, $p < 0.001$, $\text{eta}^2 = 0.02$
	SD	1.45	1.63	1.34	1.24	
Computers as safe devices	*M*	3.98	3.36	3.32	3.11	$F(3, 18723) = 298.53$, $p < 0.001$, $\text{eta}^2 = 0.05$
	SD	1.86	1.88	1.69	1.56	

Note: the differences among the clusters in categorical variables (including system data) were tested using chi-square, in scale variables, using one-way ANOVA with Tukey post hoc tests. Clusters: (1) computer owners who do not use computers personally, (2) IT technicians, (3) owners sharing the computer, and (4) sole users and seldom owners.

believe it is least safe device compared to the other clusters ($M = 3.11$; Md. = 3.00; SD = 1.56).

4.2. Country Clusters. The second cluster analysis is aimed at grouping the countries based on the results of the user clusters from the first analysis. This analysis separated four country clusters out of the 20 countries included in the data sample, which are presented in Tables 3 and 4.

Cluster 1: Western countries (Australia, Canada, United Kingdom, New Zealand, and United States). This is the cluster of the wealthiest countries in terms of GDP, and, on average, it has the highest overall network readiness index, reflected specifically in the highest number of individual Internet users, the most Internet access in households, the highest education enrollment rate, and the lowest rate of software piracy. These countries have an equal proportion of users in cluster 1 (i.e., owner, but not a user) and cluster 4 (i.e., sole users), which each represent one-third of the respondents. One-third of the people in cluster 4 are the highest proportion from all other country clusters; thus, these countries have the highest proportion of sole users and older, digitally self-efficient users. They also have the lowest representation of IT technicians and people who do not personally use the computer. Thus, this country cluster is where the overlap between the user and the software installer is the highest and the need for external help (i.e., by another family member, a friend, or a professional IT technician) is the lowest.

Cluster 2: South Africa and Israel. In terms of country-level indicators, these countries have the second highest

Table 3: Country-level variables.

Country clusters		Software installers' cluster distribution in each country (%)				Country-level indicators					
		1	2	3	4	Network readiness index (1-7)	Tertiary education (%)	Software piracy (%)	Internet—individuals (%)	Internet—households (%)	GDP per capita (Intl$)
1	Australia	35.74	6.60	24.47	33.19	5.50	86.60	21.00	84.60	86.90	49897
	Canada	33.87	5.38	25.05	35.70	5.60	na	25.00	87.10	86.60	42349
	Great Britain	36.52	4.78	22.52	36.17	5.70	56.90	24.00	91.60	89.90	40412
	New Zealand	33.89	3.02	31.88	31.21	5.50	79.70	20.00	85.50	79.80	40332
	USA	33.88	4.90	22.79	38.43	5.80	88.80	18.00	87.40	79.60	57589
	Cluster average	34.78	4.94	25.34	34.94	5.62	78.00	21.60	87.24	84.56	46115.80
2	Israel	49.23	7.69	15.90	27.18	5.40	66.30	30.00	71.50	71.50	37181
	South Africa	42.47	9.36	14.84	33.33	4.20	19.70	34.00	49.00	37.30	5280
	Cluster average	45.85	8.53	15.37	30.26	4.80	43.00	32.00	60.25	54.40	21230.50
3	Indonesia	45.40	14.21	28.13	12.26	4.00	31.30	84.00	17.10	29.10	3570
	Iran	50.60	9.58	28.28	11.54	3.70	66.00	na	39.40	44.70	5219
	Thailand	43.55	11.83	29.03	15.59	4.20	51.40	71.00	34.90	33.80	5979
	Cluster average	46.52	11.87	28.48	13.13	3.97	49.57	77.50	30.47	35.87	4922.67
4	United Arab Emirates	63.91	5.65	14.78	15.65	5.30	22.00	36.00	90.40	90.10	38518
	Bangladesh	60.55	7.03	21.10	11.31	3.30	13.40	87.00	9.60	6.50	1359
	Egypt	66.09	8.58	15.45	9.87	3.70	30.30	62.00	31.70	36.80	3479
	India	55.22	9.17	18.97	16.64	3.80	23.90	60.00	18.00	15.30	1717
	Sri Lanka	64.42	10.49	17.60	7.49	4.20	20.70	83.00	25.80	15.30	3857
	Philippines	58.97	4.58	21.37	15.08	4.00	35.80	69.00	39.70	26.90	2951
	Pakistan	57.63	7.91	20.34	14.12	3.40	10.40	85.00	13.80	13.20	1442
	Romania	53.46	8.66	15.80	22.08	4.10	52.20	62.00	54.10	60.50	9532
	Serbia	52.48	12.87	16.83	17.82	4.00	58.10	69.00	53.50	51.80	5426
	Saudi Arabia	61.72	12.50	15.63	10.16	4.80	61.10	50.00	63.70	94.00	19982
	Cluster average	58.27	9.03	18.76	13.94	4.05	34.32	67.32	39.16	40.57	8471.42

tertiary education enrollment rate and the second lowest software piracy rate. The two countries are quite different in GDP per capita, tertiary education enrollment rate, and Internet access (on both individual and household levels); Israel is higher on all these indicators. The countries in this cluster are midway between the Western countries and the other two clusters, mostly due to the high number people in cluster 4, older people using the PC, and more people installing the security software. Just under one-third of the people in these countries belong to cluster 4 (i.e., sole users), so this cluster is similar to the first. However, there are more people in cluster 1 (i.e., owner, but not a user; about half) and cluster 2 (i.e., IT technicians), suggesting that even though there are a similar number of sole users, there is a higher number of people installing the software for someone else. These two countries also have the lowest number of people who share the computer.

Cluster 3: Indonesia, Thailand, and Iran. These countries have a much lower GDP per capita than the Western countries, and they have highest software piracy rates, with quite a low rate of Internet access. We can assume that the respondents in these countries represent a very specific segment of society, with higher SES than the majority in the country. These countries have the highest proportion of users in cluster 3 (i.e., users who share the computer) of all countries, which is about 29% of the people, and also in cluster 4 (i.e., IT technicians), which is almost 12%. Together with the following country cluster (i.e., country cluster 4 below), they

Table 4: Country-level hardware indicators.

Country clusters		Software installers' cluster distribution in each country (%)				OS version (%)			CPU size (%)			
		1	2	3	4	WIN 7	WIN 8	WIN 10	Low	Low-mid	High-mid	High
1	Australia	35.74	6.60	24.47	33.19	20.5	7.9	71.6	3.2	20.1	40.0	36.8
	Canada	33.87	5.38	25.05	35.70	27.9	7.6	64.4	4.4	23.8	40.1	31.7
	Great Britain	36.52	4.78	22.52	36.17	25.0	6.2	68.8	4.5	26.8	42.0	26.7
	New Zealand	33.89	3.02	31.88	31.21	22.1	8.5	69.4	5.9	23.6	43.4	27.1
	USA	33.88	4.90	22.79	38.43	22.8	6.1	71.2	2.7	17.4	42.1	37.9
	Cluster average	34.78	4.94	25.34	34.94	23.7	7.3	69.1	4.1	22.3	41.5	32.0
2	Israel	49.23	7.69	15.90	27.18	26.5	10.6	62.8	1.4	16.4	43.2	39.1
	South Africa	42.47	9.36	14.84	33.33	34.5	15.0	50.4	6.3	31.4	41.9	20.3
	Cluster average	45.85	8.53	15.37	30.26	30.5	12.8	56.6	3.9	23.9	42.6	29.7
3	Indonesia	45.40	14.21	28.13	12.26	56.7	16.1	27.2	8.5	42.9	39.4	9.2
	Iran	50.60	9.58	28.28	11.54	48.5	26.3	25.1	5.7	27.5	52.9	14.0
	Thailand	43.55	11.83	29.03	15.59	38.8	19.6	41.6	5.0	18.5	50.4	26.1
	Cluster average	46.52	11.87	28.48	13.13	48.0	20.7	31.3	6.4	29.6	47.6	16.4
4	United Arab Emirates	63.91	5.65	14.78	15.65	39.3	19.5	41.3	6.9	23.5	49.8	19.7
	Bangladesh	60.55	7.03	21.10	11.31	61.2	14.6	24.1	6.1	30.2	49.8	13.9
	Egypt	66.09	8.58	15.45	9.87	50.5	17.5	32.0	10.3	27.0	51.4	11.3
	India	55.22	9.17	18.97	16.64	52.3	21.0	26.7	5.8	33.5	54.3	6.5
	Sri Lanka	64.42	10.49	17.60	7.49	29.7	22.1	48.2	3.4	23.9	60.7	12.0
	Philippines	58.97	4.58	21.37	15.08	49.2	16.4	34.4	11.8	38.8	38.3	11.1
	Pakistan	57.63	7.91	20.34	14.12	60.9	20.4	18.6	8.3	35.8	50.4	5.5
	Romania	53.46	8.66	15.80	22.08	48.4	15.5	36.1	5.8	34.8	38.5	21.0
	Serbia	52.48	12.87	16.83	17.82	57.3	6.0	36.8	2.7	36.6	42.0	18.8
	Saudi Arabia	61.72	12.50	15.63	10.16	48.0	19.0	33.0	4.1	25.6	49.4	20.9
	Cluster average	58.27	9.03	18.76	13.94	49.7	17.2	33.1	6.5	31.0	48.5	14.1

have the smallest amount of sole users, and they have a similar amount of people in cluster 1 (i.e., owners, but not a user) as the previous country cluster. This means that the people installing the software in these countries are mostly younger and often serve as external help for computers they do not actually use.

Cluster 4: other developing countries (Bangladesh, Egypt, India, Sri Lanka, the Philippines, Pakistan, Romania, Serbia, Saudi Arabia, and United Arab Emirates).

In terms of country-level indicators, this is the specific cluster that contains the range of countries that are more different from each other when compared to the make up of the other country clusters—some have the highest piracy rates (above 80%), yet two countries have a 50% or lower rate. Similarly, the Internet access rate is quite high in some (e.g., United Arab Emirates has 90%) but very low in others (e.g., around 14% in Pakistan). The same goes for GDP, education enrollment rate, and general NRI. We presume that each country has a different society segment for software installers. In countries with a higher Internet access rate and a higher GDP, the respondents may be closer to the population average, but, in other countries, the respondents are probably from segments that are more privileged. This is apparent, for instance, in Pakistan, which has the lowest tertiary education enrollment rate (42%) from the countries in our dataset. Yet, 86% of the respondents from Pakistan in our sample reported achieving tertiary education. The majority of respondents from these countries fall into cluster 1 (i.e., owner, but not a user). This is the highest proportion of owners, but not users, from all of the country clusters—it ranges from 53% in Romania to 66% in Egypt. With a relatively high representation of IT technicians (9%) and a low number of people from cluster 3 (i.e., users who share a computer), these countries have the widest gap between people installing and using the computer.

5. Discussion

In line with the proposed research questions, we will discuss the following: (1) who are the installers of the security software and (2) what are the clusters of countries with different patterns of security software installation.

In relation to our research questions, it is important to highlight that Windows 10 was launched in 2015 and, because we collected data between October 2016 and February 2017, many users were probably still in the process of transition to the new software. Part of Windows 10 is the Windows Security software, which includes the antivirus "Microsoft Defender Antivirus," which was previously known as Windows Defender and included in the previous

versions of Windows. By many measures, Windows Security (and Defender) could work similarly as third-party antivirus software, providing malware detection, firewall protection, and real-time threat detection. That means that not installing the third-party software does not necessarily mean a specific vulnerability. The users in our study decided to pay for a third-party software produced by ESET to protect their PCs.

5.1. Who Are the Installers of the Security Software? The four clusters that were identified in the software installer analysis reveal that the variables of computer ownership (cluster 1), professionalism (IT technicians, cluster 2), and usage pattern (i.e., shared vs. sole users, clusters 3 and 4) allow for clear distinctions between the software installer groups.

Interestingly, the largest group of software installers (cluster 1, representing 43% of the sample) are computer owners who do not use the computer. This is in line with the previous research that indicated that solving computer-related issues, such as cleaning, setting up the network, and otherwise securing it, are often dedicated to one tech-savvy person in the household or within a wider social circle known to the owner, so-called "tech gurus" or "security czars" [7, 8]. However, our large-scale research, for the first time, indicates the size of this group across different countries. These results indicate that the decision about what security software will be installed on a personal computer and its setup will often be in the hands of someone who does not use the device. And while this person most likely acts with the aim to provide a better level of security for the device user, thus aiming to reduce the risks, this person may not have a full understanding of the real skillset and knowledge of the ultimate user, thus possibly increasing the risks for bad decisions and/or actions by the end user. It is uncertain how familiar the person is with the users' needs, their online threat awareness, and their basic computer skills. This finding has several implications, as we discuss below. In general, we would like to encourage more empirical research to focus on the benefits and loopholes of the security software installation that is done by people with a different knowledge and skillset from the security software user.

The second cluster of our analyses was the installers who reported that they are IT technicians (7% of the sample). This is in line with the findings of Nthala and Flechais [6] who suggest that security decisions in the home involve both informal and business stakeholders. Our results show that the group of IT technicians is small (less than 5% in four of the 20 countries) and that probably means that informal and business stakeholders are involved as possible advisors to the computer owners and other members of the household. However, the role of the informal and business stakeholders in the process of the security software installation would require further research.

Cluster 3 consists of all of the computer users who use the computer on a shared basis (23% of the sample). This group installs the security software for themselves and for other users in the household. Most of them are computer owners (62%). The literature on the sharing of computers is quite scarce. A study on 99 households revealed that 59% of users involved someone who shared the computer to perform operations on the device, initialize accounts, or handle major configurations on behalf of the other sharer (s) [34]. Our research indicates that the sharing of the computer (and also of the security software) is quite common. However, future research is needed to understand the substance of the sharing in detail. Our study also discovered an unexpected segment of software installers that form cluster 4: sole users who seldom own the computer (27% of the sample). Respondents in this cluster are the oldest respondents in the study, with average age of about 49. They install the software on higher-quality computers, but only about a third of them are computer owners. This cluster is not covered in any related research, and it suggests the presence of a large group of aging users who are tech-savvy enough to administer their own computers. We recommend further research of this group of aging users, which will probably grow in size as the population gets older. The aging population could also have specific requirements for the security software, so software companies could develop software adapted to this group of users.

The fourth cluster has the largest proportion of females, although they still represent a minority because only about a third of installers were females in this cluster. Other clusters consist of less than 30% females, which is in line with Rode's studies (2009, 2010), where women searched for outside support more often than men, and the role of security czar belonged more often to a male family member. In our study, the lowest proportion of females was in the cluster of IT technicians (12%).

5.2. Cross-Country Differences in Installation of the Security Software. What users do with technology and what their computer skills are furthermore dependent on the wider ICT infrastructure in place at their residence and the country's overall welfare. While, in general, ICTs are more available and affordable than a decade ago, there are still wide differences according to countries, as illustrated by the Networked Readiness Index (NRI, Baller, Dutta, & Lanvin, [35]). Related work further suggests that there is a divide in security management behavior and the users' security needs between developed and developing countries (cf. [36, 37]). In a systematic literature review, Vashistha et al. [37] examined 114 publications about user security and privacy behaviors in developing countries. They argue that deficient security practices, such as ignoring security updates, are grounded in the need to save data volume, which result from economic constraints (cf. also [38, 39]). Our study also shows that people who install the security software differ between clusters of countries. The lowest need for help with online security software installation seems to be among developed countries from cluster 1 (i.e., Western countries: Australia, Canada, United Kingdom, New Zealand, and United States), by contrast to the developing countries of cluster 4 (i.e., Bangladesh, Egypt, India, Sri Lanka, the Philippines, Pakistan, Romania, Serbia, Saudi Arabia, and United Arab Emirates). The countries in cluster 1 also have the highest proportion of older users and sole users of the

computer upon which they installed the software. This seems to be another important country difference: the countries of cluster 1 (i.e., Western countries) have a more developed ICT infrastructure and a more educated older population, in contrast to other countries where aging users might struggle with computers due to insufficient education or a lack of experience with ICT.

Based on our results, it may be understood that the countries of cluster 1 (i.e., Western countries) rely more on the individual responsibility of each family member, whereas users in cluster 4 (i.e., developing countries) tend to follow more traditional models, with divided labor, where one person, typically male, is responsible for IT and IT security for the whole family. Partially, this result could be affected by the fact that the data in our database comes from the English version of the software; therefore, for some countries, the external help for installing the software may not be just because of the lack of digital skills of the person using the computer, but also due to a language barrier.

5.3. Study Limitations. The present study has several limitations. First, the study is based on cooperation with a single online security software producer. However, ESET had a 14% worldwide market share for security software in the year of the study 2016 [40] and, because of the high number of respondents, the findings are quite robust. We cannot generalize the results for all installations of the security software, but our study gives a broad and unique picture about the worldwide installations. Furthermore, the situation with security software has developed from the last six years of the data collection until now. Specifically, Microsoft developed stronger security software within Windows 10 and 11, which could impact the decisions of users about the installation of third-party software. Second, while ESET provides several language mutations for the software, we focused only on the English installations. This, however, might be one of the reasons for more need to request external help with software installation in non-English speaking countries. Similarly, the questionnaire was presented only in English, requiring at least a basic level of English from respondents, which may be rarer in some countries than in others. Therefore, the sample population could be shifted in some countries from an average inhabitant towards more educated and skilled installers of the security software who know English.

Lastly, the questionnaires were obtained from a small portion of all of the installations.

6. Conclusions and Implications

This large-scale study was conducted on data from the installations of ESET security software from software installers in 20 countries, and it shows that every other installation of security software is done by a person who will not use the computer—and that the gap between the actual user and software installer largely differs among countries. Western, more developed countries with a higher GDP and better ICT infrastructure also have the most skilled and self-efficient users who are able to install their software, as opposed to developing countries. Our study indicates that, in Western English-speaking countries, installing security software seems to be a task that is often accomplished by either the actual users or by the owner of the computer, whereas people in developing countries more often rely solely on the computer owner to install the software for other users. The findings in our study indicate a lasting digital divide on a country level. By shedding light onto the question of who installs security software, our research extends the existing body of knowledge on security practices in different countries.

The results of this study have several implications for the usage of security software, the development of security software, and the security software companies. This study revealed that security software is often installed by people who do not use the computer and the computer might be shared by more people. This implies that some steps in the setup of the security software in the installation process are done by nonusers of the computer. This should be taken into account during the software development process because the usage of the security software is related to the patterns of usage for the computer; for example, the user interface could be different for the installer and the user. It could also be different for the aging population. We point out that the investigation of the pros and cons of security software installation by persons different from the actual user would be a fruitful area for future research. Our study also shows for the first time how patterns of the security software installations differ across countries. This could help software companies to adapt different versions of the security software to relevant countries.

Data Availability

Data are not freely available because the data collection was based on cooperation with a commercial company, so there are third-party rights to data.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article. This work has received funding from the Czech Science Foundation (project no. 19-27828X).

References

[1] I. Ion, R. Reeder, and S. Consolvo, ""... No one Can Hack My Mind": comparing expert and non-expert security practices," in *Proceedings of Symposium on Usable Privacy and Security*, pp. 1–20, 2015.

[2] E. M. Redmiles, S. Kross, and M. L. Mazurek, "How I learned to be secure: a census-representative survey of security advice sources and behavior," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 666–677, 2016.

[3] J. Meisner, "Latest security intelligence report shows 24 percent of PCs are unprotected - The Official Microsoft Blog," 2013, https://blogs.microsoft.com/blog/2013/04/17/latest-security-intelligence-report-shows-24-percent-of-pcs-are-unprotected/.

[4] Statista Inc, "Windows antivirus software usage 2015 | Statistic," 2015, https://www.statista.com/statistics/507047/worldwide-windows-anti-virus-software-usage/.

[5] F. L. Levesque, J. M. Fernandez, A. Somayaji, and D. Batchelder, "National-level risk assessment: a multi-country study of malware infections," in *Proceedings of WEIS: 15th Workshop on the Economics of Information Security*, pp. 1–30, 2016.

[6] N. Nthala and I. Flechais, ""If it's urgent or it is stopping me from doing something, then I might just go straight at it": a study into home data security decisions," in *Human Aspects of Information Security, Privacy and Trust. HAS 2017*, Lecture Notes in Computer Science, T. Tryfonas, Ed., pp. 123–142, Springer, Cham, 2017.

[7] E. S. Poole, M. Chetty, T. Morgan, R. E. Grinter, and W. K. Edwards, "Computer help at home: methods and motivations for informal technical support," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 739–748, 2009.

[8] J. A. Rode, "Digital parenting: designing children's safety," in *Electronic Workshops in Computing*, pp. 244–251, 2009.

[9] E. I. Collins and J. Hinds, "Exploring workers' subjective experiences of habit formation in cyber-security: a qualitative survey," *Cyberpsychology, Behavior and Social Networking*, vol. 24, no. 9, pp. 599–604, 2021.

[10] A. P. Felt, E. Ha, S. Egelman, A. Haney, E. Chin, and D. Wagner, "Android permissions: user attention, comprehension, and behavior," in *Proceedings of the Eighth Symposium on Usable Privacy and Security - SOUPS '12*, pp. 1–14, 2012.

[11] N. S. Good, J. Grossklags, D. K. Mulligan, and J. A. Konstan, "Noticing notice: a large-scale experiment on the timing of software license agreements," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 607–616, 2007.

[12] J. Grossklags and N. Good, "Empirical studies on software notices to inform policy makers and usability designers," in *Financial Cryptography and Data Security. FC 2007*, Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds., pp. 341–355, Springer, Berlin, Heidelberg, 2007.

[13] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: a comparison of two theoretical models," *Management Science*, vol. 35, no. 8, pp. 982–1003, 1989.

[14] I. Ajzen, "The theory of planned behavior," *Organizational Behavior and Human Decision Processes*, vol. 50, no. 2, pp. 179–211, 1991.

[15] E. M. Rogers, *Diffusion of Innovations*, The Free Press, New York, 4th edition, 1995.

[16] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change1," *The Journal of Psychology*, vol. 91, no. 1, pp. 93–114, 1975.

[17] A. E. Howe, I. Ray, M. Roberts, M. Urbanska, and Z. Byrne, "The psychology of security for the home computer user," in *2012 IEEE Symposium on Security and Privacy*, pp. 209–223, 2012.

[18] P. Seuwou, E. Banissi, and G. Ubakanma, "User acceptance of information technology: a critical review of technology acceptance models and the decision to invest in information security," in *Global Security, Safety and Sustainability - The Security Challenges of the Connected World. ICGS3 2017*, vol. 630 of Communications in Computer and Information Science, pp. 230–251, Springer, Cham, 2016.

[19] M. Warkentin, J. Shropshire, and A. Johnston, "The IT security adoption conundrum: an initial step toward validation of applicable measures," in *AMCIS 2007 Proceedings*, p. 276, 2007.

[20] N. Nthala and I. Flechais, "Informal support networks: an investigation into home data security practices," *Fourteenth Symposium on Usable Privacy and Security ({SOUPS}*, 2018, pp. 63–82, 2018.

[21] E. M. Redmiles, S. Kross, and M. L. Mazurek, "Where is the digital divide?: a survey of security, privacy, and socioeconomics," in *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pp. 931–936, 2017.

[22] J. A. Rode, "The roles that make the domestic work," in *Proceedings of the 2010 ACM conference on Computer supported cooperative work - CSCW '10*, pp. 381–390, 2010.

[23] S. Kiesler, B. Zdaniuk, V. Lundmark, and R. Kraut, "Troubles with the Internet: the dynamics of help at home," *Human-computer interaction*, vol. 15, no. 4, pp. 323–351, 2000.

[24] R. E. Grinter, W. K. Edwards, M. W. Newman, and N. Ducheneaut, "The work to make a home network work," in *The Work to Make a Home Network Work*, ECSCW 2005, H. Gellersen, K. Schmidt, M. Beaudouin-Lafon, and W. Mackay, Eds., pp. 469–488, Springer, Dordrecht, 2005.

[25] N. Thompson, T. J. McGill, and X. Wang, ""Security begins at home": determinants of home computer and mobile device security behavior," *Computers & Security*, vol. 70, pp. 376–391, 2017.

[26] J. Cohen, *Statistical Power Analysis for the Behavioral Sciences*, Lawrence Erlbaum Associates, Hillsdale, N.J, 2009.

[27] D. Burt, P. Nicholas, K. Sullivan, T. Scoles, and S. Ghernaouti-Helie, *The Cyber Security Risk Paradox-Impact of Social, Economic, and Technological Factors on Rates of Malware. Microsoft Security Intelligence Report Special Edition*, Microsoft Corporation, Redmond, WA, 2014.

[28] G. Mezzour, K. M. Carley, and L. R. Carley, "An empirical study of global malware encounters," in *Proceedings of the 2015 Symposium and Bootcamp on the Science of Security*, pp. 8:1–8:11, 2015.

[29] V. S. Subrahmanian, M. Ovelgonne, T. Dumitras, and B. A. Prakash, *The Global Cyber-Vulnerability Report*, Springer International Publishing, Switzerland, 2015.

[30] World Bank, "GDP per capita," 2016, https://data.worldbank.org/indicator/NY.GDP.PCAP.CD.

[31] World Economic Forum, "The global information technology report 2016," 2016, http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf.

[32] D. B. Henry, P. H. Tolan, and D. Gorman-Smith, "Cluster analysis in family psychology research," *Journal of Family Psychology*, vol. 19, no. 1, pp. 121–132, 2005.

[33] M. Sarstedt and E. Mooi, "A concise guide to market research," *The Process, Data, and, 12*, 2014.

[34] T. Matthews, K. Liao, A. Turner, M. Berkovich, R. Reeder, and S. Consolvo, ""She'll just grab any device that's closer": a study of everyday device & account sharing in households," in *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, pp. 5921–5932, 2016.

[35] S. Baller, S. Dutta, and B. Lanvin, *Global information technology report 2016*, Ouranos, Geneva, 2016.

[36] Y. Ben-David, S. Hasan, J. Pal et al., "Computing security in the developing world: a case for multidisciplinary research," in *Proceedings of the 5th ACM workshop on Networked systems for developing regions - NSDR '11*, pp. 39–44, 2011.

[37] A. Vashistha, R. Anderson, and S. Mare, "Examining security and privacy research in developing regions," in *Proceedings of the 1st ACM SIGCAS Conference on Computing and Sustainable Societies*, p. 25, 2018.

[38] M. Chetty, R. Banks, A. J. Brush, J. Donner, and R. Grinter, "You're capped: understanding the effects of bandwidth caps on broadband use in the home," in *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 3021–3030, 2012.

[39] A. Mathur, B. Schlotfeldt, and M. Chetty, "A mixed-methods study of mobile users' data usage practices in South Africa," in *Proceedings of the 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing - UbiComp '15*, pp. 1209–1220, 2015.

[40] OPsoftwareAT Inc, "Windows anti-malware market share report," 2017, https://metadefender.opswat.com/reports/anti-malware-market-share#!/?date=2017-10-28.