Cyber threats in Israel between the years 2010-2019 : social, economic and security aspects, according to online press articles / Haya Steinberg

Abstract

The purpose of this study is to examine, for the first time in a comprehensive and in-depth manner, the cyber threats in the State of Israel in the decade 2010-2019, as presented by the online news press: to explore the main issues of cyber threats, as reflected in the digital press, while creating an integrative and holistic picture of the factors that shape and influence them, and their advertising and marketing patterns.

The basic research questions were: The threat, the threatened party and the threatening party – characteristics, influential factors in the context in which the threats occurred, and the relationship between the virtual and physical environment in the context of cyber threats; Technology used by the threatening party; Discovery of the threat and the punishment – how much time elapsed from the beginning of the threat to its discovery and treatment, the factors and/or those responsible for the discovery of the threat, and the characteristics of the punishment or its absence; The advertising and marketing patterns of cyber threats in the online press.

The research was based on qualitative analysis – content analysis according to categories of articles from the online press that deal with cybercrime. The study was based on the online newspapers Haaretz, Ynet, Walla, Maariv, People & Computers, Calcalist, Mako, Globes and TheMarker. The reason for choosing these sites was their popularity among the Israeli public, as seen in their high viewing percentages. The articles were collected from the news websites, creating a variety from the years to which the study pertains, and through the use of keywords and tags that have become broader, on the one hand, and have become more accurate, on the other. The analysis was carried out in stages: in the process of collecting the articles described above, initially, approximately 3,800 articles were collected, concerning approximately 194 cases. According to an initial sorting

of the cases (and the articles), several basic broad categories of cyber threats were built – social threat, security threat, economic threat, political threat, geopolitical threat and ecological threat. In the next stage, the cases in these categories were examined by analyzing those articles that deal with these cases in a focused manner, and in this way, subcategories were built. For example, the subcategories pedophilia and shaming belong to the social threat category. The number of articles in each of the categories and subcategories was then examined. Following this examination, the three categories of cyber threats with the largest number of articles – social threat, security threat and economic threat – were kept, while the other categories were removed. In the three remaining categories, the ten subcategories that had the largest number of reviews were kept, while the rest of the subcategories were removed. This was done both because of the overly broad scope of the articles that were accepted, and out of a desire to get a picture of the salient characteristics of cyber threats in the State of Israel. According to the categories and subcategories that remained after the filtering process described above, a category tree was built to map the relationships: horizontal between categories, vertical between categories and their subcategories. The subcategories express characteristics of the categories above them. In the next step, three cases were chosen from each of the ten subcategories to represent that subcategory. The criteria for selecting the cases were: their maximum number of reviews, reviews from various years throughout the decade in question, and having distinct characteristics of that subcategory. In this way, 1,021 articles, 30 cases (three cases from each of the ten sub-categories) were analyzed in depth and in detail.

The process described above was carried out in its entirety while examining the theoretical and research literature and reports from Israel and the world, and during a characterization and conceptualization process that became diverse, focused and more precise, on the one hand, and broad, general and theoretical, on the other.

After analyzing the findings, we came to the following conclusions:

The findings of the study reveal a variety of social, economic and security cyber threats topics that are covered by the online news press. However, the presence of social threats is very noticeable, encompassing more than half of the publications. Also notable is the large number of publications dealing with incitement and shaming of various kinds, reported in over 60% of the publications.

Another notable finding is the significant impact of concrete events [such as Yassin Abu Al-Kara's decision to carry out a stabbing attack at the central station in Jerusalem, among other things, following Trump's statement a few days before on his recognition of Jerusalem as the capital of the State of Israel (security threat - Lone-wolf attacks)], as well as the general reality atmosphere, on the threats. They determine them, and influence their character and strength. This is evident in threats of incitement, such as incitement against elected officials and senior officials in the governing bodies, and other social issues, but also in security issues, such as individuals attacks, and sometimes even economic ones, such as the cyber threat in the Leumi Card case - Eliran Rosens, the threatening person, was an internal factor - A former employee of the organization, and his act was motivated, as he described by his feeling of injustice at not being promoted. According to the research findings, it appears that these effects are not sufficiently addressed. Future research that focuses on this issue may contribute to finding more effective solutions and ways of dealing with cyber threats in the State of Israel, in the immediate and long term.

Prominent findings on the issue of the technological means used by the threatening elements: Among the social networks, Facebook is used the most; An extensive effect of anonymity – mainly through the use of fake identities – on the extent and damages of cybercrime in a variety of fields, is evident; The deep web, mainly databases of companies and organizations that have permission to collect sensitive personal information about people, is often used for economic crime (the Leumi Card case), when the threatening elements are internal, that is, past and/or present employees of the company or organization; The research findings also show the intolerable ease of availability of offensive technological means.

There is also a blurring of boundaries regarding the technologies used by the threatening elements: a spillover in the use of social networks from social cyber threats to economic and security threats [such as the use of Facebook in the case of posing as seductive young women (security threat - cyber espionage)]; The lack of separation between the civil and security space in the technological platforms, on which the threat is applied; An interesting finding concerning the technological means used for cybercrime. Despite the differentiation between legitimate technological means and those whose purpose is offensive, it seems that even the legitimate tools (such as social networks, platforms for running campaigns, mobile phones, etc.) are used by cybercrime controllers. The blurring of boundaries creates confusion and makes it difficult to deal with

cybercrime. Studies that will examine and redefine the boundaries reflected in the present reality may contribute to a more effective treatment of crime in the digital space.

It was also found in the current study that, due to the large number of users in the digital space, on the one hand, and, on the other, the anonymity and lack of sufficient supervision and cooperation in this arena, many of the cybercrimes were discovered a long time after they were committed, sometimes years later, if at all, and therefore were often characterized by multiple offenses and victims. Moreover, when they were discovered, it was often at the hands of one of those involved, usually the victims and/or their relatives, and in the minority of cases by the enforcement authorities. It was also found that in quite a few cases there was no punishment, usually for crimes of incitement and, prominently, in those cases involving ruling political parties, and in cases where the threatening parties were found physically in another country – a possibility that characterizes cyber threats and makes enforcement activities difficult.

From examining the contents of the publications, several factors that affect the coverage degree of the topics and cases emerged. Those that drive Extensive coverage, such as, dealing with various polarization issues in Israeli society, spreading lies and half-truths while using emotional manipulations to influence the public's consciousness (social engineering), many reactions, and those that drive little coverage of cases, such as, security issues, or, few covered cases, in issues, such as, economic threats to central infrastructures. In this context, the absence of threats, dealing with certain topics, from the study, due to their lack of coverage in sufficient quantity that would result in their inclusion in it, despite their high frequency, is notable. Indeed, the decision whether to include subjects in the study stems from the extent of their coverage. Among those not included: women trafficking and gambling. The scarcity of coverage of these threats impairs the possibility of bringing them into the public discourse and addressing them in the best possible way. These findings indicate a picture of threats obtained from the coverage, which does not always faithfully reflect reality, rather, the interests of those holding positions of power of various kinds. Perhaps more studies should be directed to the relationship between the presence of various issues in the news information to which the public is exposed and the exclusion of problems related to these issues, as well as, of disadvantaged populations.

Some of the findings of this study are consistent with what is written in the theoretical literature on cyber threats. However, some of the findings reflect the unique content of cybercrime in the arena and context of the State of Israel, with its social, security, political and geopolitical complexity. Moreover, they occasionally allude to gaps between the cyber threats in the State of Israel and the information about them made available to the public through the various news websites.

MMS Number: 9926962111405776