Psychosocial Approach to Cyber Threat Intelligence

Kitty Kioskli
City, University of London, Department of Computer Science, United Kingdom, EC1V 0HB and Gruppo Maggioli, Research & Development Lab, A. Papandreou 19, 151 24, Marousi, Greece

Nineta Polemi
University of Piraeus, Department of Informatics, Karaoli and Dimitriou 80, Piraeus, 185 34 and FORTH external expert, Athens, Greece

Abstract

Cyber attackers continuously show new levels of intention by performing more sophisticated attacks on networks and important infrastructures (e.g., hospitals). This is an urgent situation calling for a swift improvement for cyber defenders. Hence, a paradigm shift is necessary to ameliorate the effectiveness of current practices. Behavioural, social and psychological related information about the attackers is considered in this paper, important elements of the Cyber Threat Intelligence (CTI) that improve cyber defense practices. The aims of this paper are to firstly provide a review of relevant behavioural and social theories and models that can be used for better capturing the attackers' characteristics and then to utilize them by giving insights on more realistic security measurements.

1. Introduction

These Cyber Threat Intelligence (CTI) is information about threats and attackers (also called cybercriminals, cyber agents, hackers, adversaries). This information helps to analyze attacks and vulnerabilities, to estimate attack potential and risk levels and further select effective controls and mitigation actions to protect our infrastructures, assets (physical and cyber) and digital ecosystems [1].

CTI is a natural requirement for all successful cybersecurity risk assessment and management efforts as well as for situational awareness and cybersecurity incident handling practices. Related security management standards (e.g., ISO31000, ISO2700x, ISO15408, ISO18045 [2]) and methodologies (e.g., OCTAVE, EBIOS, TVRA, OWASP, NIST-800, MITRE) also require useful information and insights for all security measurements in the steps of threat/vulnerability analysis, risk assessment, selection of mitigation actions (controls). For example, for estimating the vulnerability level (weakness) of an asset we need to know how easy the asset can be exploited or what is the attack potential, which in return requires information about the attackers' capabilities.

The concept of attack potential is introduced in ISO/IEC 15408-1:2009, NIST [3] as the effort needed for an asset to be attacked, in terms of an attacker's expertise, resources and motivation. The psychological and behavioural dimensions of the attacker are not considered in the traditional measurements of the attack potential. In fact, these dimensions are not taken into account in any other security measurement (e.g., threat/vulnerability/risk levels) or in the selection of mitigation actions and controls. Efforts to classify and identify the attackers are limited to considering motivations and abstract capability levels [4].

In our previous work [5], we adopted a socio-technical approach to our security efforts by further analyzing the attackers' characteristics and profiles. In particular, in [5], we proposed a social-technical approach in calculating the vulnerability and cybersecurity risks where the quantifiable psychological profile became a factor in the calculations. In [6], we extended our approach to demonstrate how the extended profile of the attacker can be used for estimating more accurately the attack potential. In this paper, we will review existing theories and models and present our overall socio-technical CTI model in order to achieve more realistic security measurements. Demonstration scenarios from the health sector have been selected as an attempt to contribute to the acknowledged need [7] to enhance the protection of our health critical infrastructures (e.g., hospitals) and medical assets (e.g., medical devices, health records).

2. Behaviour and Social Theories

Research efforts [8] are being conducted, in combating cybercrime study technical and human factors, to determine cybercriminal behaviours. This is achieved by using multidisciplinary approaches from various scientific domains (e.g., social sciences, criminology, anthropology, cyberpsychology).

Behavioural scientists claim that there is not adequate knowledge about the behaviour of the user (whether legitimate or illegal) in relation to Information Technologies (IT) in general, and specifically in relation to cybersecurity of IT [9]. However, psychologists and social scientists, have sought ways to explain the users' behaviour towards cybersecurity through a number of theories. These theories, which are described below, can be used in the cybersecurity domain. In particular behavioural and psychosocial data is an efficient way to be proactive in cyber defense and are useful to identify and explain the behaviour of attackers as we propose in this paper.

To start with, normative theories are essential for the study of informal argumentation, decision-making and judgement. It remains complicated to identify the suitable norms to be assigned to a behaviour, especially when ignoring the origins of normativity [10]. In the context of cybersecurity, the secure behaviour of a legitimate user towards an IT system needs to be defined as well as the norms of the secure behaviour so we can use them as point of reference to identify abnormal (abusive behaviour) towards the IT system. Furthermore, according to the normative theories, the origin of normativity, which in our case is the legitimate user with safe behaviour towards the IT system, need to be studied and identify his/her characteristics. This is why it still ambiguous -what exactly makes something normative- until we identify the specific norms. According to this theory, it looks like a rational human behaviour occurs when this behaviour pairs with a criterion and logic to assess arguments. There are obvious limitations to logic, as highlighted by the Bayesian probability which calculates argument strength, making the Bayesian appropriate for the normativity's requirements [10]. In the cybersecurity context, this may translate that the secure behaviour of a user will depend upon explaining all the security processes (arguments) which need to be followed. A user will assess and adopt these arguments depending upon his capabilities to understand and apply these processes and will depend upon his social values (e.g., ethical, philosophical, cultural).

Another broadly used theory is the Theory of Planned Behaviour (TPB; Figure 1). TPB utilizes a predictive model, which shows that attitudes and subjective norms affect behavioural intention, and intention influences actual behaviour. The TPB suggests that individuals' behavioural intention is a valid predictor of their actual behaviour. For example, an IT user with intention to go against the social norms (e.g., does not follow procedures, restrictions, laws, common practices) will most probably not follow the security practices required, making the individual a dangerous user for the security of the IT system, or even worse a potential attacker.

The facet of behaviour is subjective norm. While, how easy or difficult is to perform a behaviour depicts the perceived behavioural control [11].

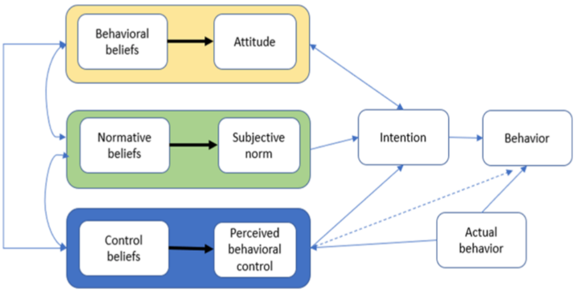

Figure 1. Theory of Planned Behaviour [12]

Broadly speaking, the stronger the perceived behavioural control, the subjective norms and the attitude the greater the person's intention to express the anticipated behaviour. The person's attitude is strongly connected to its behavioural, normative and control beliefs. For example, if an IT user believes he controls his illegal behaviour by performing only minor illegal actions (perceived behavioural control), and he/she is surrounded by a group of people encouraging him/her to perform more (subjective norm), e.g., Dark Web hackers' friends and he/she gradually acts on it (attitude) then this IT user will be very much likely to continue performing illegal behaviours (e.g., not respect security procedures) to an extent that he/she may become an attacker. Although research into subjective norms in relation to cybersecurity is sparse, since is mostly used in health-related behaviours, there is some evidence showing its validity in security threat analysis as well. It will be helpful to investigate the modifiable behavioural factors involved, identify which have the greatest predictive value and then feed them to an interdisciplinary framework or a threat detection system. For example, TPB has been successfully used to predict online protective behaviours [13]. These findings reveal a strong relationship between intention and a subjective norm and indicate that external parties (i.e., manager) influence his IT employees to commit cyber protective behaviours.

To continue with, a widely used theory is also the Social Cognition Theory (SCT) [14] which was firstly introduced as a social learning theory and suggests that cognitive factors are strongly associated to behavioural and environmental factors (Figure 2). According to SCT, there is a cause-and-effect relationship between an individual's behaviour and the social world and an individual's characteristics. Therefore, criminal or abnormal behaviour can be learnt like any other type of behaviour. An example in the cybersecurity context would be that an illegal behaviour (e.g., attack an IT system/digital asset) is affected by the individual's knowledge about the weaknesses (vulnerabilities) of the targets (IT system/asset) (Personal/Cognitive factors), peer-pressure from his/her social group, e.g., regional /political party, hackers' group in Dark

Web (Environmental factor) and his/her own ability (skills, knowledge, computing power) to perform the attack (Behavioural factor).

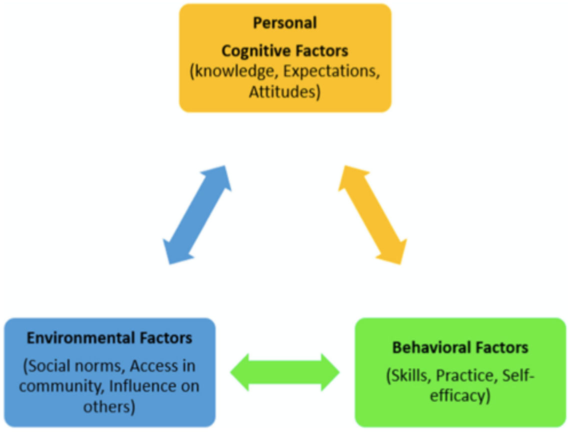
Personal
Cognitive Factors
(knowledge, Expectations, Attitudes)
Environmental Factors
(Social norms, Access in community, Influence on others)
Behavioral Factors
(Skills, Practice, Self-efficacy)

Figure 2. Social Cognition Theory [15]

To complement the SCT comes Social Bond Theory [16] which assumes that weaker social bonds may increase the possibility of an individual to become involved in an illegal action. SCT is interested in explaining how behaviour is maintained, compared to other theories focusing on what initiated the behaviour, and can be used in the cybersecurity field to explore decision support and behaviour. For example, by investigating the impact of self-efficacy (behavioural factor) may explain the decision-making process in cyber behaviour. Self-efficacy may be described as self-evaluation which is significant in a person's behaviour and may influence the self-regulation, amount of effort, handling of obstacles and initiation of tasks [15].

3. Models of Psychosocial Attackers' Profiles

Psychological profiling is defined as the various methods of identifying and analysing behaviours executed in a crime. Although psychological profiling is common, mostly in forensic psychology, aiming to sketch a criminal's profile, the implementation in cybersecurity crimes and cybersecurity attacks appear to be relevant as well. Various taxonomies of attackers are found in the literature [e.g., 17] with a number of characteristics and motives. Cyberpsychology, investigative psychology research and behavioural science, have supplied accurate profiling models for attackers based on their personality traits [e.g., 17] by developing the Five-Factor Theory (FFT) model [18]. The FFT incorporates five main traits (Table 1) which are greatly affected by factors such as, genes', environmental and genetic ones.

Table 1. Facets of The Fft Model [18]

Traits	Facet Example
Agreeableness	Trust
Extraversion	Positive emotions
Conscientiousness	Self-efficacy
Neuroticism	Self-consciousness
Openness to experiences	Ability to express emotions

There is also Fogg's behavioural model [19] which is a model describing the likelihood of a Behaviour (B) occurring is a product of Motivation (M), Ability (A), and the appropriate Trigger (T). Fogg's behavioural model is referred as the B=MAT model (Figure 3) and is used to manage the behaviour related to defending organizations and help employees become more security aware and follow appropriate cybersecurity practices. However, in this paper, we utilize this model in order to capture the attackers' general behavioural traits.

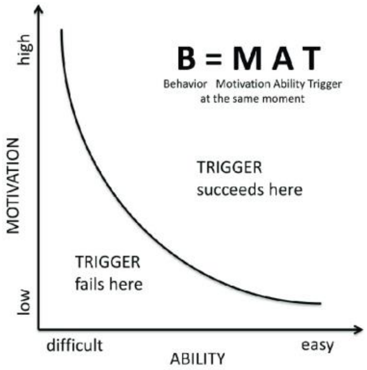

Figure 3. Fogg's Behavioural Model [19]

Extended psychological profiles for attackers have been developed using other factors as well, such as intelligence, social and technical skills [3,4]. Various cybersecurity threat models also consider attackers' classifications and basic behaviour traits in their analysis. Also, psychologists and behavioural analysts use different approaches to measure personality and psychosocial traits of an individual. Psychological and cognitive assessments provide useful data which contribute towards the understanding of a person's capabilities and characteristics. These data are collected and interpreted through various methods such as rating scales and interviews. NIST and MITRE adopt the rating scale approach and suggest a set of attack factors (characteristics) according to their capability, intention and target to describe an attacker. However, the above-mentioned approaches described in this section do not consider psychological and behavioural characteristics as potential attack factors.

In our previous work [5,6] we have proposed a multi-dimensional, measurable attackers' profile and its personality traits based upon psychological, behavioural, societal, technical ability and personality traits using the FFT model and Fogg's behavioural model. In this paper, we enhance the characteristics that play a crucial role in adopting an attacker's behaviour, as we see in the following Table 2.

Table 2. Attackers' Characteristics

Personality Traits	**Description & Examples**
Extraversion	Gregariousness (e.g., Social engagement in attackers' groups) Assertiveness/Outspokenness (e.g., Leadership skills) Activity/Energy level (e.g., Enjoys a busy life) Positive Emotions/Mood (e.g., Happiness)
Conscientiousness	Orderliness/Neatness (e.g., Well-organized) Striving/Perseverance (e.g., Aims to achieve excellence) Self-Discipline (e.g., Persistent engagement to goals) Dutifulness/Carefulness (e.g., Strong sense of duty) Self-Efficacy (e.g., Confidence to achieve goals)
Openness to experiences	Intellect/Creativity Imaginative (e.g., Intellectual style) Scientifically Interested/Originality (e.g., Evidence-based) Adventurousness (e.g., Experiences of different things)
Cognition	Knowledge (e.g., Collecting information for the topic of interest) Expectations (e.g., Evaluating strengths and possible outcomes) Attitudes (e.g., Acting based on knowledge and expectations)
Social - Behavioural Traits	**Description & Examples**
Selected social exposure	Difficult to adapt to conventional social norms (e.g., Events) Easy to build virtual anonymous, professional relationships (e.g., Using anonymous identity has contacts with other attackers in the Deep Web) Easy to build strong e-bonds in hacking communities (e.g., These communities are closed to the public)
Not conventional relationships	Difficult to build physical relationships or contacts Easy to build professional (with other attackers) virtual, anonymous relationships under their moral code (us versus them approach)
Not talkative	Difficult to initiate small casual talks or social talks Difficult to express him/herself
Manipulative	Easy manipulating people via electronic means (e.g., phishing)
Technical Traits	**Description & Examples**
Networking skills	Knowledge in network architectures, systems, functional and operational aspects (e.g., DNS, HCP)
IT skills	Competencies in operating systems (e.g., languages, software and emerging technologies, programming)
Soft skills	Problem Solver (e.g. Understand, analyze and solve difficult problems) Social observer (e.g., Audits security behaviours)
Forensics skills	Know how to use security scripts, forensics tools (e.g., Intrusion detection/penetration tools)
Available resources	Available computing power (e.g., Owns/access to high computer processing power), devices, time, economic support security communities
Privileges	Insider (e.g., Works in the organization with significant /limited/no access) Outsider (e.g., supply chain partner with significant limited/no access) Outsider-Third party (e.g., vendor/manufacturer with indirect or
Targeted Knowledge	Information/ measurements gathered about the targets (e.g., CVSS), knowledge in effective attacks
Motivational & Social Traits	**Description & Examples**
Political	Political power (e.g., Espionage, fake news)
Personal	Personal satisfaction, feeling of accomplishment, boredom, competition, economic gain
Cultural	Whistleblower (warns of any digital wrongdoings)
Philosophical	Humanitarian/activist/ theological goals (e.g., Stealing for societal benefit)

Trigger Traits	Description & Examples
Vulnerable assets	Open ports (e.g., Zero-day vulnerability) New non-certified technologies (e.g., App, AI systems)
Human weaknesses/errors	Vulnerable infrastructures (e.g., No access control in data center) Unintentional human error (e.g., Distracted administrator) Intentional human error (e.g., Reckless but knowledge of risk)

Developing and scoring the attackers' profiles, based on the characteristics in Table 2, is a complex task since an appropriate metric system (measurements and weights) will need to be considered for each trait. A trustworthy, applicable scoring system will need to be a result from multi-disciplinary efforts between various sciences (behavioural, security, psychology, criminology, anthropology, cyberpsychology, mathematics etc.) based upon evidence-based high-quality studies and surveys. As a first attempt, to demonstrate the connection with the attacker potential we provide a general, rough scoring approach (Table 3) based upon the NIST measurements ([3]-Appendix D).

The attacker profile can be used in providing more realistic security estimates and measurements. This will be described in more details in the next section.

Table 3: Attackers' Profile

Qualitative Values	Semi-Quantitative Values		Attackers' profile
Sophisticated (multi-sectoral expert)	96-100	10	More than 96% of each of the Traits in each category in Table 2
Experienced	80-95	8	More than 80% of each of the Traits in each category in Table 2
Moderate	21-79	5	More than 21% of each of the Traits in each category in Table 2
Basic	5-20	2	More than 5% of each of the Traits in each category in Table 2
Insufficient	1-4	0	Less than 5% of the Traits in each category in Table 2

The attacker profile can be used in providing more realistic security estimates and measurements. This will be described in more details in the next section.

4. Socio-technical Security Estimates

The attackers' profiles (Table 3) will be used to estimate the attack potential, the vulnerability and risk levels. In particular, will lead us to a scoring of the attack potential (AP) following the ISO/IEC 18045 [4] values as seen in Table 4.

Table 4: Scoring Attack Potential (Ap)

AP Qualitative Values	AP quantitative values	Description
Beyond High	10	Sophisticated Profile (multi-sectoral expert)
High	8	Experienced Profile
Moderate	5	Moderate Profile
Basic	2	Basic Profile
Very Low	0	Insufficient Profile

The AP depends upon the attackers' profile. For example, an attacker with a sophisticated profile (e.g., nation-state actor, cyber-terrorist), strong motivation (e.g., commercial espionage) to attack a medical device (e.g., new insulin pump with glucose monitoring utilizing wireless communication links), who has the technical skills (e.g., hardware security) and available resources (e.g., hardware and software radio platform), we need to assume that he/she/they will be capable to develop the means to execute and succeed in attacking the medical device or develop significant offensive capabilities (AP will be Beyond High). The attacker's profile score indicates the likelihood of a person to adopt the behaviour of an attacker where the AP score indicates the likelihood of carrying out an attack.

Let us consider also the under-development health care platform ONCORELIEF (Figure 4), where patients use it to continuously monitor their health and to receive recommendations from the physician. The health data are collected in the sensing framework feeding a health application reaching the back-end database (db) where health records and medical data of the patients are stored and processed. The caregivers and doctors also provide additional medical data about the patient via the health application and a web interface. The potential of the health records to be stolen (attack) from the back end medical db (asset) will depend upon the attacker's profile enabling him to overcome the installed security controls of the platform e.g., there is a high possibility for an experienced attacker (see Tables 2, 3) to carry out the attack and steal the health records in the medical db (AP= High).

Another important security measurement is the vulnerability (weakness) level of an asset (e.g., medical db) to a specific threat (e.g., non-authorized access). The vulnerability level, $I(V_i)$, using classical methodologies, as we saw in our previous work [5,6] take into consideration the following four (4) vulnerability factors (VFi) (see Figure 4).

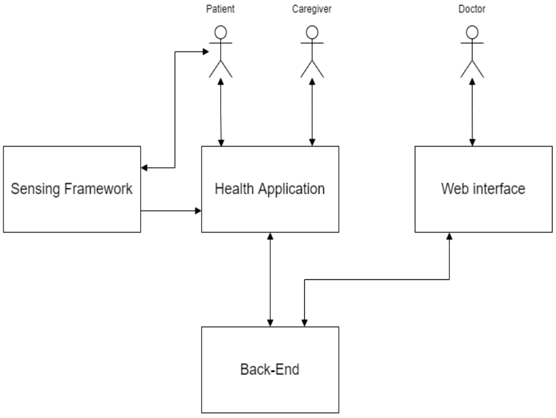

Figure 4: Oncorelief Platform [7]

- VF1: Ease of discovery which is related to how easy is to discover the vulnerability/weakness. Four possible score values can be found here: practically impossible (0), difficult (1), easy (2) and very easy (3).

- VF2: Ease of exploit that actually depicts how easy is for an adversary to exploit the vulnerability/weakness. The score values for this factor are the following: practically impossible (0), difficult (1), easy (2) and very easy (3).

- VF3: Ease of detection meaning how likely is for a threat to be detected. The likelihood of detection scores as follows: proactively detectable (0), actively detectable (1), post-actively detectable (2) and non-detectable (3).

- VF4: Awareness which depicts how well-known is a vulnerability/weakness. The score values for this factor are: totally unknown (0), hidden (1), obvious (2) and publicly known (3).

The authors claimed in [5,6] that all above vulnerability factors depend upon the attackers' profile, thus the attackers' profile score needs to be considered as a new vulnerability factor namely factor, VF5. The level of a vulnerability, $l(V_i)$, was computed [5] based on five (5) vulnerability factors, VF_j, as follows:

$$l(V_i) = VF_5\left(\sum_{j=1}^{4} VF_j\right). \qquad (1)$$

The above calculation led to estimate the risk of a threat T_i to an asset A as:

$$R'_A(T_i) = l(T_i)l(I_i)l(V_i) = l(T_i)\, l(I_i)\, VF_5\left(\sum_{j=1}^{4} VF_j\right), \qquad (2)$$

where $l(T_i)$ notes the threat level (frequency or likehood of treat occurrence, $l(I_i)$ the impact level (consequences/damages that will reveal if a threat occurs) and $l(V_i)$ the vulnerability level of threat T_i to the asset A.

Formula 2 reveals that the risk level depends upon the attacker's profile as well. For example, the risk for the medical db (asset A) to be accessed illegally (the threat here is the non-authorized access) will depend upon the attacker's profile as well.

Another important security score is the CVSS [20] that describes the criticality of the vulnerability and depends upon the exploitability factors of the vulnerabilities; in particular, CVSS depends upon all five factors (VF1-VF5). It also depends upon the impact of the vulnerability to the standard security dimensions (confidentiality, integrity, availability). Thus, the CVSS score also depends upon the attacker's profile, VF5.

To conclude the security measurements, depend upon the attackers' profiles and thus different profiles of potential attackers indicate different security measurements. The higher the score of the attacker's profile, the higher the security measurements (attack potential, vulnerability level, risk level, CVSS).

5. Conclusions and Future Work

New emerging cybersecurity threats and attacks call to advance our CTI capabilities. The human nature, behaviour and actions make the individual the prime enabler of the cybersecurity attacks and we need to consider his/her characteristics as a crucial part of the CTI which can advance our cyber defense practices.

Considering human factors and parameters will enhance our expertise in estimating attacks' potential and cyber risks. Therefore, by considering these factors and collaborating with all experts in the relevant fields (sociology, psychology, criminology, security, behavioural sciences) will provide the necessary paradigm swift which will become so vital to boost the effectiveness of existing cyber defense methods and techniques, improve our cyber resilience and reduce cyberattack incidents.

This paper was a first attempt to quantify social characteristics and use them in security measurements to achieve more realistic security estimates. However, collaborative further research efforts are needed to enhance the methodologies (based on social sciences research instruments) that will provide appropriate metrics and measurements (qualitative and quantitative) of attackers' characteristics that will lead to more accurate attackers' quantified profiles.

Furthermore, EU security directives and initiatives (e.g., Cybersecurity Act, NIS, eIDAS) adopt solely a technical approach as well. The authors would propose to consider a broader socio-technical view that may increase social applicability and acceptance of the security policies.

6. References

[1] ENISA (2018) 'Exploring the opportunities and limitations of current Threat Intelligence Platforms' https://www.enisa.europa.eu/publications/exploringthe-opportunities-and-limitations-of-current-threatintelligence-platforms (Access Date: 1 January, 2021).

[2] ISO/IEC 27001 (2013) 'Information technology - Security techniques - Information security management systems - Requirements' https://www.iso.org/standard/54534.html (Access Date: 20 December, 2020).

[3] National Institute of Standards and Technology (2012) 'Guide for Conducting Risk Assessments' https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (15 November, 2020).

[4] ENISA (2013) 'ENISA Threat Landscape midyear 2013' https://www.enisa.europa.eu/publications/enisa-threat-landscape-mid-year-2013 (Access Date: 15 December, 2020).

[5] K. Kioskli, N. Polemi, "A socio-technical approach to cyber risk assessment." International Journal of Electrical and Computer Engineering. 2020;14(10), pp. 305-309.

[6] K. Kioskli, N. Polemi, "Measuring psychosocial and behavioural factors improves attack potential estimates." In Proceedings of the 15th International Conference for Internet Technology and Secured Transactions. 2021, pp. 216-219.

[7] ONCORELIEF (2020) 'A digital guardian angel enhancing cancer patient's wellbeing and health status improvement following treatment' https://cordis.europa.eu/project/id/875392 (Access Date: 12 January, 2021).

[8] CC-DRIVER (2020) 'Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour A Research' https://cordis.europa.eu/project/id/883543 (Access Date: 12 January, 2021).

[9] T. Dinev, Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies." Journal of the Association for Information Systems. 2007;8(7), pp.386-408.

[10] A. Corner, U. Hahn, "Normative theories of argumentation: Are some norms better than others?" Synthese. 2013;190(16), pp.3579-3610.

[11] A. Icek, "The theory of planned behavior". Organizational Behavior and Human Decision Processes. 1991;50 (2), pp.179-211.

[12] A. Icek, (2019) 'Theory of Planned Behavior Diagram.' http://people.umass.edu/ aizen/tpb.diag.html (13 December 2020).

[13] S. Burns, L. Roberts, "Applying the Theory of Planned Behaviour to predicting online safety behaviour." Crime Prevention and Community Safety. 2013;15(1), pp.48-64.

[14] A. Bandura, "Social foundations of thought and action: a social cognitive theory." 1986, Englewood Cliffs, N.J.: Prentice-Hall.

[15] A.B. Hardy, G. Howells, A. Bandura, N.E. Adams, "Tests of the generality of self-efficacy theory." Cognitive Therapy and Research. 1980; 4(1), pp.39-66.

[16] J. Chriss. "The Functions of The Social Bond." The Sociological Quarterly. 2007;48(4), pp.689-712.

[17] A. Matulessy, N.H. Humaira, "Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits." Psychology and Behavioral Sciences. 2016;5(1), pp.137-142.

[18] R.R. McCrae, P.T. Costa, "Validation of the five-factor model of personality across instruments and observers." Journal of Personality and Social Psychology.1987;52(1), pp.81-90.

[19] B.J. Fogg, "A behavior model for persuasive design." In Proceedings of the 4th international Conference on Persuasive Technology. 2009; p.40.

[20] Common Vulnerability Scoring System https://www.first.org/cvss/v3-1/cvss-v31specification_r1.p df (Access Date: 20 January, 2021).

7. Acknowledgment

The research conducted in this paper was triggered by the authors' involvement in the projects OncoRelief [7] and CC-Driver [8]. The authors are grateful for the financial support of these projects that have received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreements No 875392 and No 883543 respectively. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.