IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 13 May 2023, accepted 4 June 2023, date of publication 7 June 2023, date of current version 16 June 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3283791

RESEARCH ARTICLE

What Will the Future of Cybersecurity Bring Us, and Will It Be Ethical? The Hunt for the Black Swans of Cybersecurity Ethics

ALEKSANDRA PAWLICKA[1,2], MAREK PAWLICKI[1,3], RAFAŁ KOZIK[1,3], AND MICHAŁ CHORAŚ[1,3,4]

[1]ITTI, 61-612 Poznań, Poland
[2]Faculty of Applied Linguistics, University of Warsaw, 00-927 Warsaw, Poland
[3]Institute of Telecommunications and Computer Science, Bydgoszcz University of Science and Technology, 85-796 Bydgoszcz, Poland
[4]Faculty of Mathematics and Computer Science, FernUniversität Hagen, 58097 Hagen, Germany

Corresponding author: Aleksandra Pawlicka (apawlicka@itti.com.pl)

This work is funded under the APPRAISE Project – fAcilitating Public & Private secuRity operAtors to mitigate terrorIsm Scenarios against soft targEts, with the support of the European Commission and the Horizon 2020 Programme, under Grant Agreement No. 101021981.

ABSTRACT Although the ethics of cybersecurity might seem to be simple, the matter can be surprisingly complicated. This paper discusses the results of an extensive study aimed at uncovering the anticipated, emerging ethical issues related to cybersecurity. First, it discusses the ''strong signals'', i.e., the ''mainstream'' worries and concerns. Then, it uncovers the ''weak signals'' - the hidden, less-discussed concerns, which may still define the upcoming future of the ethics of cybersecurity. The results of the study are also compared to the outcomes of a similar experiment conducted two years ago, in order to see if the upcoming ethical dilemmas anticipated back then have in fact become a reality.

INDEX TERMS Cybersecurity, ethical issues, ethics, weak signals.

I. INTRODUCTION

Ethics aim at determining what is wrong and what is right, and setting up standards of acceptable, moral behaviors in certain situations. Cybersecurity directly affects people's well-being; this is why ethics play a prominent role in it. In the context of cybersecurity, ethical principles are in fact at the core of cybersecurity practices, as they refer to responsible use of technologies, in order to protect individuals and ensure they live well [1], [2], [3], [4]. Although the ethics of cybersecurity might seem to be simple - protect the data of good guys, do not let the bad guys in - it can be surprisingly complicated [5]. This paper discusses the results of a broad Horizon Scanning campaign aimed at uncovering the anticipated, emerging ethical issues related to cybersecurity.

II. BACKGROUND - WHY CAN CYBERSECURITY ETHICS BE SO COMPLEX?

Unlike other experts whose professions give them plenty of power, and whose fields of expertise affect people's lives, such as healthcare professionals or lawyers, the professionals who deal with cybersecurity do not have an established, universal code of conduct yet [1]. Naturally, there are a number of laws which regulate how to navigate cybersecurity; but legal does not necessarily mean ethical [5]. It has been discussed that even if such a code was created, it would never fit all the cybersecurity-related contexts. Rather, the guidelines and procedures should be tailored to the activities and challenges of a given practice [6].

Despite the lack of a universal code of conduct, there have been some suggestions of the principles that the ethical cybersecurity should be built upon. One such set has been proposed by Formosa et al. and encompasses:

- Beneficence; i.e., cybersecurity being used to make people's lives better.
- Non-maleficence, that is not using cybersecurity technologies to do any sort of intentional harm.
- Autonomy - using technologies in such a way that human's autonomy is respected and protected.
- Justice, i.e., promoting fairness, equality and impartiality instead of discrimination or preventing equal access.

The associate editor coordinating the review of this manuscript and approving it for publication was Tyson Brooks.

- Explicability, that is using technologies in a transparent and comprehensible way [7].

Another, more straightforward approach has been employed by Van Impe, who proposed these commandments:

- ''Do not use a computer to harm other people.
- Protect society and the common good.
- Be trustworthy, meaning only enter commitments you can keep, and uphold trusted connections with people.
- Have a plan for coordinated vulnerability disclosure.
- Respect human rights.
- Disclose data on a need-to-know basis and maintain privacy.
- Comply with legal standards.'' [8]

With the constant emergence and development of new technologies, cybersecurity evolves as well. While this in general brings new advantages and opportunities to the society, it also often gives rise to new, unprecedented adverse phenomena and vulnerabilities [2]. This means that new ethical challenges arise, too [9]. The outbreak of the COVID-19 pandemic, and the accompanying shift in the significance of digital technologies has too sparked further dialogue on the issues of cybersecurity and its ethics [10], [11].

Technologies as such are never ethically neutral; rather, they mirror the values of their designers, vendors and users [6]. The knowledge of the possible ethical problems is crucial for both the cybersecurity professionals and users alike, in order to be prepared for them. Knowing what may happen and how others handled similar situations may help solve dilemmas if and when they arise [5]. This is why it is crucial to comprehensively scrutinize the ethical issues related to cybersecurity in a regular manner, and concentrate on both the ethical dilemmas that have already been confronted, and the possible, anticipated issues that are yet to arise. This paper presents the outcome of such a study.

III. MATERIALS AND METHODS - STUDY DESIGN

This work showcases the results of a follow-up to the 2019-2020 horizon scanning study which was described in [10] and [12]. The study aimed at finding the emerging ethical dilemmas related to cybersecurity.

In order to find out whether the anticipated future dilemmas have changed or not, and if any of them had already become a reality, another study was conducted in April-October 2022. It aimed at examining the new sources, the opinions in which were given after the first study was completed.

A. HORIZON SCANNING

The horizon scanning study was selected as the method of choice. It was decided that this technique would be the best one for obtaining this kind of answers.

Horizon Scanning is a foresight process. There exist several definitions of the technique, ranging from the ''attempt to systematically imagine the future in order to better plan a response'' [13], a ''systematic examination of sources to detect early signs of important developments'' [14] or the means of evaluating ''the importance of 'things to come''' [15]. It aims at uncovering the ''weak'' signals, i.e., the ones which are not commonly known or discussed, which are not among the ''mainstream'' concerns. The method has been known for several decades. It started with commercial organizations from a variety of sectors, but was later adopted by public bodies as well. The main objective of a study of this kind is to supplement the process of planning, be it research, funding or policymaking one.

Generally, Horizon Scanning has been used in relation to the early lifecycle of technologies; it is often employed to check for challenges, opportunities, or to grasp trends in a broad manner. It does not study the ''signals'' in great depth; rather, it is there to provide early warnings.

Horizon Scanning, unlike a survey, does not rely solely on scientific papers and book chapters. Instead, a multitude of sources are scanned, including (but not limited to):

- professional press
- non-scientific books (including grey literature),
- patents,
- the news media,
- meetings/conference proceedings,
- government bodies' reports,
- surveys,
- the social media,
- blogs,
- wikis. . . [16].

There is no universal framework of Horizon Scanning. Instead, the adopted model should take into account the peculiarities of the scanned sector; hence, a number of models have been described in the subject literature. The choice of the scanning method is also up to the researcher and their needs; typically more than one method is applied, either sequentially or in parallel [15].

B. THE COURSE OF THE STUDY

The study design followed the general principles described in [12], with the necessary modifications taking into account the experience and expertise gained over the years following the initial study, as well as the conclusions drawn from it. Specifically, the search strings consisted of the combinations of three keywords, from the following three groups:

Group 1:

- cybersecurity
- cyber security
- cybercrime
- cyber crime

Group 2:

- ethics
- ethic
- ethical
- fundamental rights
- human rights

Group 3:

- concern
- controversy
- issue
- issues
- matter
- problem
- question

Then, the results of the search were initially scanned by the researchers performing the study, to check whether they may potentially be of interest. As the search results tend to be noisy, they were analyzed by the researchers until they remained relevant. After removing duplicates, 4298 various items were taken into consideration. On top if that, several hundred social media posts (Twitter, Facebook, Instagram, YouTube), sourced using the same criteria were analyzed. In total, 319 items were selected for an in-depth analysis. The types of content included: books and book chapters, reports, whitepapers, magazines, various websites, blogposts, curricula, webinars, opinion videos, and comment sections. In this study, a number of scientific articles and book chapters were also taken into consideration if they seemed interesting; however, as it turned out in the first study, they rarely deviate from the mainstream and the ''strong signals'', so they were not the main interest of the study.

Subsequently, the main ethical concerns/issues/dilemmas discussed in the selected sources were extracted. All of them were used to build the word cloud (Fig. 2); the most interesting and relevant findings have been discussed in detail below.

IV. RESULTS - THE FINDINGS

A. THE OLD FINDINGS

Figure 1 summarizes the findings of the first study. As visible, most of the ethical concerns identified in it pertained to the various aspects of privacy. Other strong(er) signals encompassed the questions of freedom of speech, freedom of expression, surveillance and censorship.

In turn, although the 2022 study highlighted the issue of privacy as the most important one, the second most popular ethical dilemma has changed. As seen in Figure 2, the question of the so-called ethical hacking has received a great deal of interest. The issues of bias and consent have also been discussed in multiple sources. The identified strong and weak signals have been discussed in greater detail below.

B. THE "STRONG SIGNALS", OR THE "MAINSTREAM" ETHICAL ISSUES OF CYBERSECURITY

1) STRONG SIGNAL 1: PRIVACY

The majority of sources deem users' privacy as the main ethical issue related to cybersecurity. Some of the most common and serious threats to privacy are leaks, breaches and misuse of data [17]. In order to secure data privacy, organizations need to tackle its most prominent challenges, that is treating data privacy not as an afterthought, but as an inseparable aspect of data collection, taking into account the legal regulations, such as GDPR [18] or the California Consumer Privacy Act, but also the variety of devices and access point, especially in case of remote work and bring-your-own-device policies in place, and scaling the measures to the ever-growing amounts of processed data [19], [20]. Experts notice that the new laws have indeed given the users a bigger say in what happens to their data; however, there is still a lot to be done as far as aligning business' strategy of companies in order not to infringe on the users' privacy [21].

The issue with cybersecurity is that the practices, aimed at protecting valuable data and assets, often infringe on people's privacy as well. Finding the equilibrium between people's need for security and protecting their privacy may prove to be real struggle. In order to achieve this, the concept of people's dignity is essential, which includes people's right to privacy, and confidentiality itself as something which should be respected [22]. Data privacy is such a burning question, as the concerns about it do not pertain to cybercriminals only; just the opposite, the cybersecurity experts should respect the users' privacy, too. This can be problematic, as keeping information safe from hackers sometimes requires losing privacy from some other party, for example, one that is responsible for monitoring the data. Sometimes even, the objectives of cybersecurity and privacy seem to collide. The question arises: what is the amount information that cybersecurity experts can see in the name of ensuring security compliance before it stops being ethical? [5], [23] Again, cybersecurity professionals are thought to be the first to defend against breaches and other cyberthreats, and consequently, they are trusted to protect users' privacy. If the experts do not do their work carefully enough, e.g., they use outdated encryption, or their practices are otherwise poor, it is deeply unethical [1].

2) STRONG SIGNAL 2: ETHICAL HACKING, ETHICAL HACKERS

Ethical hackers, also known as white hat hackers, are cybersecurity experts who are tasked with breaking into systems in order to uncover any security vulnerabilities it may have. The main difference between white hats and ''conventional'' cybersec experts is that the former concentrate of finding the system's vulnerabilities whilst the latter concentrate mostly on preventing attacks and unauthorized access [24].

It is said that attacking your system yourself is the best way of checking if it is able to withstand a cyberattack [25]. This way, not only the vulnerabilities can be uncovered and removed, but also the staff can be appropriately trained. Yet, employing ethical hackers, as well as their mere existence, give rise to a number of ethical dilemmas.

First of all, there is the question of trust between the organization and the hacker. The organization assumes that the white hat they employ has the adequate experience, training and will not to harm to them. There are now various courses which provide ethical hacking certification; there is no official licensing system in place yet, though [26]. The critical line which differentiates ethical hackers from threat

FIGURE 1. The summary of the signals identified in the first study.

actors is that the white hats follow ethics. The basic necessary principles they have to follow are: doing no harm, staying legal, keeping within the agreed upon boundaries, reporting the found vulnerabilities, and respecting data sensitivity and confidentiality [27].

Some ethical dilemmas related to ethical hackers is that what they should do if, when performing a simulated attack, they uncover forbidden, illegal materials on the client's hard drive. If, for example, when being tasked to hack a system, they find child pornography there, should they keep it a secret for the confidentiality's sake, or report it to the authorities? [28].

3) STRONG SIGNAL 3: BIASED AI DECISIONS

The ''very real'' ethical issues around the biased AI cybersecurity algorithms are mentioned again. They must be tackled in order not to affect the whole progress of AI and trust [21]. When it comes to employing artificial intelligence (AI)/ machine learning (ML) in cybersecurity, some people wonder whether artificial intelligence should be even used in the first place. Yet, cybercriminals have no ethics, and they use AI with malicious intent. If defenders do not use AI to defend systems, cyberthreat actors are far more likely to win. In fact, the risks of not using AI are far greater than the issues related to AI itself. Thus, in the context of cybersecurity, ''the use of AI is not only ethical but morally imperative.'' [29].

Another problem is that although technology should be value neutral, algorithms are only as smart as the data they were trained on [30], i.e., if the dataset contains racial, gender or any other kind of prejudice, the bias will be reflected in the algorithmic output. In cybersecurity, it is particularly important to rid of any potential bias, as it may have serious real-life impacts, like in the case of faulty facial recognition algorithms which led to arrests of innocent people in the USA [31].

One of the measures taken in order to get rid of the ethical dilemmas if to follow the principles of AI explainability and fairness [32], [33].

4) OTHER STRONG(ER) SIGNALS

Other ethical dilemmas of cybersecurity that were identified previously pertain to the ethical use of data. It is generally agreed upon that the handling of data should always base on empathy, i.e., remembering that it is a person who is involved and affected by data; prioritizing data ownership and control, by letting the users make decisions on their personal boundaries of data use; being transparent in relation to how much and what the data is collected for; taking accountability for the security of data; and preserving equality, by ridding of any prejudice or bias that might have driven the data collection process [19], [32].

There is the ethical duty to disclose vulnerabilities or risks once they have been identified, so that the affected parties can make their decisions and act accordingly (for example, a company having a vulnerability in their system must let their customers know about it) [34]. As there is no one-size-fits-all solution, each organization must develop their own practice, with the ethical principles in mind [3].

The ethical dilemmas related to the ransomware attacks have also been extensively discussed, as during the pandemic the number of ransomware attacks has drastically risen [12]. The biggest ethical dilemma is whether one should pay

FIGURE 2. The summary of the signals identified in the second study.

ransom to cybercriminals. Naturally, this seems to be the easiest way to get the data back (provided the criminals will hold up their end of bargain). Yet, reinforcing the behavior will only encourage criminals to go on with their actions and demand even bigger amounts of money. Then, there have been propositions to make paying ransom illegal - would it be ethical, though? If payments were against the law, it could further punish the victims of ransomware attacks who were simply willing to get their stolen data back [35].

C. THE "WEAK SIGNALS" - THE ANTICIPATED, EMERGING ETHICAL ISSUES OF CYBERSECURITY

This section presents the most interesting findings of the study - the ''weak signals'' of the anticipated ethical issues of cybersecurity.

Firstly, the new, state-of-the-art technologies, such as IoT and Cloud Computing, have also posed an array of cybersecurity-related ethical dilemmas, which keep emerging with the development and progression of the technologies.

1) HIDDEN/WEAK SIGNAL 1: INTERNET OF THINGS-RELATED ETHICAL ISSUES OF CYBERSECURITY

First and foremost, the cybersecurity-related ethical dilemmas of the cybersecurity of the Internet of Things (IoT) also pertain to the users' privacy. The users often are not aware what kind of data and how much of it is collected by the devices [36]. The risk of the devices being compromised is rising, as they are heavily interconnected and many of them have been reported to be very easily hacked (as in the case of hackable baby monitors). And as the IoT devices are prevalent in our daily lives, they may collect very personal and intimate details. Thus, the smart devices, if hacked, may indicate e.g. when we are home and when not - which poses another serious security risk. Also, the data collected by the devices also has a great market value.

In many cases, the users are required to give their consent, and decide what to share and what not to share before they can even turn their devices on, which is ethical - but who cares to ensure that the users are tech-savvy enough to understand what they are really consenting to? In this context, it is also unethical if the Terms and Conditions are written in a technical jargon or prolonged artificially, so that they are less understandable.

There are security threats of the IoT which may not be easily manageable, or manageable at all - in some cases it is enough to change a password, but what if it is an IoT-enabled cardiac implant that gets compromised? In addition to that, such a breach may be life-threatening if a hacker forces it to administer irregular pacing, or switches the device off completely.

Another noteworthy ethical issue is the question of who is responsible for ensuring proper cybersecurity of the IoT devices - regulators, retailers, manufacturers, or maybe the users themselves. The regulators and governments are not able to keep up with the pace the new threats/ technologies in cybersecurity emerge. Retailers do not design the devices and do not install safety precautions themselves. On the other hand it may be against the manufacturers' interest to apply too strict security measures.

Lastly, with how the technology is progressing, we may not be able not to use IoT in the future - so the issues of cybersecurity and the related ethical dilemmas must be solved as soon as possible.

2) HIDDEN/WEAK SIGNAL 2: CLOUD COMPUTING AND ITS CYBERSECURITY

A broad range of the cloud computing-related cybersecurity ethical issues stem from the fact that it is not always clear who is the owner of the data once it ''goes cloud''. First of all, the question arises if the users, once they decide to use a cloud service, retain ownership of the information, especially in the cases when the data is generated using the service, or the provider can claim ownership of the data, too. This dilemma is also related to the issue of various jurisdiction and laws which may be based on the location of the server rather than the user. These considerations relate to cybersecurity as they would influence the outcome of a data breach. These dilemmas, in turn, are strongly intertwined with the questions of informed consent.

The risk of potential intrusions has additional dimensions with cloud computing - a breach into a cloud service does not affect one user, but a multitude of people. Yet, as [9] notice, this technology brings so many advantages that when considering its ethics, the users are often able to accept the potential small harms that come with it.

3) OTHER HIDDEN/WEAK SIGNALS

In this section, the identified hidden/ weak signals (herein referred to as HWS) have been discussed in alphabetical order.

HWS3: Admitting when you are not powerful enough.

No matter how much money is spent on cybersecurity, the government itself does not possess enough power to test all their networks and asset. In this case, the help of devoted ethical hackers is a must in order to improve the country's cyber-defense capabilities. It would be unethical if the government did not admit that and as a result, did not ask for the support from the skilled experts [37].

HWS4: AI in security leads to arms race

Another concern related to the use of AI/ML in cybersecurity is that employing AI in cybersecurity actively contributes to the arms race with threat actors. The ethical dilemma here is whether to use the AI tools for cybersecurity or let criminals gain the upper hand by doing nothing [29].

HWS5: Bad for business?

Some business owners are said to be reluctant to employ cybersecurity measures as they may interrupt the business procedures or cause inconvenience to customers or workers. Yet, as the proper maintenance of the security system is as significant as providing the services to the customers, this too becomes the question of ethics [38].

HWS6: Children and cybersecurity

Owing to the number of children who use Internet every day, and the even lower age at which they start using Internet-enabled devices, it is crucial to instill the principles of cybersecurity in them. Additionally, in the times of the COVID-19 pandemic, online classes became the new reality all over the world. This is why children must be made aware of the potential dangers that using the Internet brings.

It is also the parents' responsibility to routinely check on children's devices and ensure their safety, even if it may seem to be counter-intuitive wrt parenting. Although it may not seem to be easy, children should also be taught cyber-ethics. This will both keep them safe online and help them grow and develop further IT competencies in the future [39].

HWS7: Data ownership

With device and software evolution, the amount and types of data collected has drastically increased. The data may then be used to profile the users and predict their behaviors. Even if the profile is built entirely by means of artificial intelligence algorithms, all the ''subsequent actions are intentional'' [40].

HWS8: Ethical cybersecurity research

Ethical way of conducting research has been mentioned before; generally, scientists are expected to follow the ethical principles by default. Over the centuries, the ethical dilemma of whether the results justify the means has been raised innumerable times. Yet, there still happen the situations which cause a public outcry, like the case of the researchers from the University of Minnesota, who admitted to systematically sneaking critical vulnerabilities into the Linux Kernel code base, and wrote an article about it - all in the name of research. It was all the more shocking as they did so without the users' consent to become the proverbial guinea pigs. The researchers kept on performing these non-consensual tests until being called out by the community. As the researchers did not take the responsibility for what they did, the whole university got banned from the Linux Kernel group. As Kaufmann asks, the question arises whether in case of cybersecurity research the ends justify the means, and how to obtain consent if it may influence the findings [27].

HWS9: Health tracking

With health tracking, there exists the dilemma of whether organizations ought to create ''digital twins'' in code, in order to experiment on them. This also applies to the healthcare-services-related cybersecurity, as the ''twin'' may be exploited in a number of ways [41].

HWS10: Inevitable shortfall of cybersecurity staff

Some sources express the worry that the pace of digital transformation and development of technologies do not go hand in hand with the available cybersecurity talent, knowledge and expertise; thus, managing cyber risk is becoming an increasingly challenging task [42].

HWS11: Intrusive advertising

Advertisement campaigns are also seen as violating basic human rights, by invading the customers' privacy [43]. Another issue relates to the fact that for the sake of personalized ads, companies also collect data in order to track and profile users, and sell the information to data brokers [44].

HWS12: Lack of empathy

This issue is related to penetration/phishing or other attack simulations aimed at testing the unaware employees of a company. The approach that blames, belittles or even punishes the people who failed the tests is does not empower them to change their behavior. Instead, the testees have to be approached in an empathetic, understanding way [45].

HWS13: Misinformation, disinformation and Deep Fakes

In the context of cybersecurity, there is the worry that disinformation, and most notably the deep fake technology, will be increasingly used in order to invade people's privacy, misuse their identity, phish their personal information, and so on [41].

HWS14: Monetizing the culture of fear.

With the omnipresence of digital threats and the vast attack and threat actor catalogues, it is easy to instill panic or fear, both in individual end-users and organizations. It has been mentioned that some security consultants may be very eager to play on that and make their clients spend much more money that it is necessary. The ethical dilemma which arises here is whether charging large sums is exploitation or just how free market works [6]. A similar moral dilemma is when a cybersecurity expert promises more than they are able to achieve, or even manipulates data for the sake of earning more, as it is possible to make a network more secure, but never completely secure [6].

A similar issue relates to what companies say about their actions towards securing the data they handle, what they actually do, and if it is proportional to the value of the data, especially in the cases of big companies which collect vast amounts of sensitive and personal data, and they attract the cybercriminals' attention [44].

HWS15: Neurotechnology

The state-of-the-art advances of neurotechnology make it now possible to change a person's behavior or thought patterns [41]. While this itself is a source of ethical dilemmas, it also raises a lot of cybersecurity-related issues.

With neurotechnologies, it is crucial to ensure that patients enjoy their full advantages whilst the potential harm is minimized. The chief concern is the patients' data and privacy security, especially in the cases when the sensitive data is recorded and stored. Patients must be aware of what data can be extrapolated from their neural information collected and express their personal boundaries concerning the scope of the collected info.

If the devices can be hacked, which can also result in interrupting therapy, the cybersecurity measures must be imposed hospital-wide and with regard to the patients linked to the network. Manufacturers have to be held accountable for identifying and ridding of possible vulnerabilities [46].

HWS16: No Internet for you

What Russia has been doing in the ongoing war in Ukraine, as well as the situations in China or Iran have shown that restricting or preventing the access to the Internet may become a powerful means of controlling a nation or keeping the citizens in a bubble of information which the government is favorable of. The aforementioned countries have been known to oppose democratic values, so what they are doing with the Internet access comes as no surprise. Still, what about other countries? Can we be sure that they will not/do not keep us in information bubbles, partially by means of cybersecurity technologies?

HWS17: Quantum computers

There are voices worrying that various threat actors, including nation-states will soon employ quantum computers in order to crack the existing encryption mechanisms. This in turn will lead to a severe disruption to all the services which rely on encryption, such as the financial sector, e-commerce, and so on. The blockchain-based technologies will be vulnerable to this kind of attacks as well. If organizations do not switch to post-quantum cryptography quickly enough, it will lead to a major disaster. The ethical approach to this situation includes preparing for it - a.k.a. becoming ''crypto-agile'' - by adopting the security mechanisms once they become available [47].

HWS18: Quis custodiet ipsos custodes?

This Latin phrase, which translates into ''who watches the watchers'', refers to the situations when security teams interfere with other legitimate operations including hacking, like in the case of the Google security team shutting down a counterterrorist operation conducted by a Western government. The fact that Google not only decided to stop the operation but also made it public has raised a lot of ethical controversy [48].

HWS19: Phishing dilemma

Specifically, the phishing readiness tests have sparked controversy, when the messages to the employees were crafted in order to resemble an e-mail from the finance and payroll department of a company, with the promise of paying them a bonus for their contribution in the times of the COVID-19 pandemic. The link in the message led to a simulating phishing exercise. The particular incident was criticized as taking the test too far, as using such an emotive bait it resulted in upsetting the employees and breaking trust and the sense of security amongst them, thus undermining the cybersecurity efforts. If a phishing test is to be successful training, not tricking, it may not be thought of just as a ''gotcha'' exercise. Even if the results of the exercise are not satisfactory, they should be turned into a learning experience, by providing the staff with helpful, engaging feedback, not punishment [45].

HWS20: Resource allocation

Cybersecurity measures cost a lot of money, owing to the number of resources they require, such as time, expertise or skilled personnel. Yet, consequences of the lack of adequate cybersecurity measures often entail much higher costs. The situation in which the lack of balance between allocating funds for anything else and well-resourced cybersecurity is an ethical issue too, especially when people's life and well-being is at stake (e.g., in a hospital) [3].

HWS21: Testing new technologies.

Actually, all the new cybersecurity-related technologies should be tested with ethics in mind, i.e., taking into account the possible risks to the users. With new, emerging technologies, the risks may not be anticipated by the experts, simply because they have not been dealt with before. Another point to consider is that although the direct participants may have expressed their consent, the tests may pose indirect risks to other related parties [9].

HWS22: To teach or not to teach (cybersecurity)?

Another signal related to cybersecurity ethics is the ways it is taught. Cybersecurity as a subject is quite unique, as the practical skills a student learns may be directly related to an illegal activity, no matter if they do it just out of curiosity, or with malicious intent. It is also not always clear whether the students (this is particularly true in the case of online courses) are not based in companies or even countries which support global cybercrime or are openly against democratic values, like Russia or China [49], [50]. These concerns may lead to the question if cybersecurity/ hacking should be even taught at all.

This is why teachers and instructors teaching cybersecurity should put emphasis on the questions of ethics, and teach ''liberal'', democratic values alongside them. This way, the students are empowered with the ability to think critically about what they do and what the consequences of these actions may be, rather than having to bear with the repercussions and regret after it is too late. Another suggestion is not to teach ''the whole story'' and let the students figure the rest out themselves, and show them the test dummy sites which let students practice their newly acquired skills without breaking the law [49], [51].

''There is too much potential to do harm, deliberately or through unintended consequences of decisions made, in our craft to send them out without an understanding of ethical issues and how to address them. (. . .) I cannot tell [the students] what to think, but they ought to know how they reached their own conclusions and whatever they decided to do, be able to do it on purpose not just drift into it unthinking.'' (comment by m.robertson8_291084, in [49].

HWS23: The environmental impact of cybersecurity

The growing need for cybersecurity measures generates a greater demand for computing power in order to process the incoming data as quickly and efficiently as possible. This consumes vast amounts of energy. The ethical dilemma here is striking the balance between saving energy and ensuring the best cybersecurity possible [21].

HWS24: The ethics of cybersecurity experts and how to recruit them.

''Cybersecurity professionals have an obligation to both their organizations and the general public to carry out their duties ethically. It's crucial to know where to draw the moral line and stay ethically sound while aiming to better the security of any network they are protecting.'' [1]

Actually, cybersecurity experts have to possess the same knowledge and skills as their criminal counterparts - i.e., a cybersecurity professional should know how to copy credit card data, infiltrate users' data and so on. Therefore, they are able to do it as well. As the safety of the users'/ customers' critical data is in the hands of the cybersecurity experts, they must demonstrate to their supervisors that they are able to handle it. The cybersecurity professionals also deal with private, sensitive, or proprietary data and they have to adhere to the ''butler's credo'' - always keep what they see strictly confidential, no matter how juicy the gossip they found on a client's hard drive may be.

As there exist no straightforward, generally recognized certification or accreditation, it usually must be demonstrated by the experts' behavior. It is generally advised for the supervisors to demonstrate ethical behaviors so that the workers adopt them as well. It is also considered to be the ethical responsibility of the employers to recruit the staff who is not going to take advantage of their unique power. In other words, it is not enough to concentrate on the technical skills of a candidate; the employers should have their staff's moral standards in mind, too [22], [38].

HWS25: . . .and workforce in general

Workforce faces a number of various cyber-dangers, such as hacking, identity and data theft, data breaches, phishing, and so on. They have to be made to practice digital hygiene, which in turn contributes to better cyber ethics and improved cybersecurity [52].

HWS27: Unequal access to cybersecurity

Just like the general unequal access to the Internet, the lack of equality when it comes to access to cybersecurity is a serious ethical issue.

HWS28: Vigilante ''testers'', rouge white-hackers and scientist Searching for vulnerabilities is an inseparable part of developing products. However, the tests performed without consent are dangerously similar to cybercrime. Some hackers, who do not work for any organizations, may feel the urge to perform simulated attacks and search for system vulnerabilities by themselves. Whilst they may be well-motivated and have good intentions only, this may be the source of many ethical issues. First of all, they usually do not ask permission to hack into systems. Then, if they do uncover a vulnerability, they may be tempted to monetize it in an illegal manner, which shifts them from white to black hats [53]. Another issue is related to the situations when they found vulnerabilities but the organization does nothing to fix it - should the hackers announce it publicly, in order to warn people? [5], [27]

HWS29: Weaponization of technology

A.k.a. can we trust technology to ''fight a war for us'' [41]?

HWS30: Whistle-blowers' issues

The first and foremost question concerning whistleblowing is the most general one - is it ethical? Edward Snowden, when revealing thousands of documents proving massive invasion of privacy, had to violate contracts and break the law to expose it. For almost a decade, the public has come to a satisfactory conclusion whether this was ethical or not. Cybersecurity faces very similar dilemmas - for example, if a cybersecurity experts finds a harmful vulnerability a company does not want to fix. Is it ethical to violate the contract with the client and break the business' privacy in order to warn the users whose privacy might be in danger? [5]

As new regulations were put in place, concerns have been expressed wondering if the incentives from regulators could

FIGURE 3. The hidden/weak signals - the anticipated emerging ethical issues of cybersecurity.

lead to an increase in cyber-whistleblowing, i.e., people being able to report all forms of cyber misconduct, such as data breaches or vulnerabilities in systems, and being protected by law.

Without proper mechanisms in place for dealing with reports in an ethical way, as by nature cyber-whistleblowing differs from other complaints and poses different challenges, each company should determine how to react to cybersecurity-related whistleblowing, who is responsible for handling the complaints, and de facto ''identify and address potential concerns before they become full-blown whistleblower complaints, which can then take on a life of their own'' [54].

HWS31: When security turns into surveillance

''This is where I think one of the key ethical dimensions comes in. How one treats intelligence activity or law enforcement activity driven under democratic oversight within a lawfully elected representative government is very different from that of an authoritarian regime. Or is it?'' [48]

There are voices against too many cybersecurity measures, as it may be used by governments for mass surveillance, e.g., like in the case of facial recognition systems, which are said to compromise fundamental privacy rights of citizens [55]. In such cases, when there is lack of balance between privacy and security, the same platforms and technologies believed to be able to foster democracy and security are used against exposed citizens [56].

HWS32: Zero-day trading

Another ethical dilemma related to cybersecurity may be the question of trading zero-day exploits. There have existed companies that pay hackers to disclose found

software vulnerabilities to them, rather than to the vendors. The companies are supposed to protect the affected users before the vendors fix the problem. While this seems to be a very ethical thing to do, there have been documented cases when such companies were contacted by wealthy ''contractors'' who offered to buy the bugs for substantial amounts of money and urged to do it in secret. As Madsen remarks, ''buying 0-days is something every single country does now, (. . .) that includes your country as well.'' Since zero-day exploits have even been used by nation states attacking other ones, vulnerability researchers have to make ethical decisions concerning who they are selling the bugs to, and if money can buy everything [57].

Figure 3 shows the identified hidden/weak signals - the anticipated emerging cybersecurity-related ethical issues.

V. CONCLUSION

This paper has presented the results of a broad study of the anticipated, emerging cybersecurity-related ethical issues. The outcome of this follow-up study shows that data, technology and cybersecurity are living things [58]. They continuously evolve, and so do the accompanying ethical issues. The development of technology will lead to the rise of even more, new ethical dilemmas [59]. In the span of two years between the studies, there has been a noticeable shift in the most pressing ethical dilemmas of cybersecurity. The results presented in this paper can thus contribute to drawing the attention to the most urgent problems and provide the starting point for both the discussions on the matter and taking immediate, targeted actions.

As cybersecurity has broad implications for management, each major decision should be made in accordance with ethical standards. The same system can bring either benefit or harm, depending on the ethics underlying its application [34]. Consequently, the discussion on the ethical dilemmas of cybersecurity must continue, and the list has to be updated, preferably in the form of an inter- and multidisciplinary dialogue [60]. Then, the outcomes of the discussions have to be transformed into meaningful actions [61].

The future will tell if the worries come true and the anticipated ethical dilemmas related to cybersecurity become mainstream, or if we are in for even more surprises.

REFERENCES

[1] *Cybersecurity Ethics*, DC Encompass, Barangaroo, NSW, Australia, 2021.

[2] M. Martin. (2022). Ethical & Security Issues in Information System. Guru99. Accessed: Feb. 4, 2023. [Online]. Available: https://www.guru99.com/mis-ethical-social-issue.html#3

[3] *A Holistic Approach to Ethical Issues in Cyber Security*, Swiss Cyber Inst., Zürich, Switzerland, 2021.

[4] A. Pawlicka, M. Pawlicki, R. Kozik, and R. S. Choraś, ''A systematic review of recommender systems and their applications in cybersecurity,'' *Sensors*, vol. 21, no. 15, p. 5248, Aug. 2021.

[5] Z. Amos. (2022). The Difficult Ethics of Cybersecurity. ReHack. Accessed: Feb. 4, 2023. [Online]. Available: https://rehack.com/security/the-difficult-ethics-of-cybersecurity/

[6] Andcom. (2023). Chapter 5—Compliance, Ethical and Professional Issues in Cybersecurity. ERASMUS. Accessed: Feb. 4, 2023. [Online]. Available: https://andcom.erasmus.site/courses/module-5-cybersecurity-as-basic-necessity-of-every-learning-process/lessons/chapter-4-cyber-security-threat-prevention-and-best-practices/

[7] P. Formosa, M. Wilson, and D. Richards, ''A principlist framework for cybersecurity ethics,'' *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102382.

[8] K. Van Impe. (2021). Cybersecurity Ethics: Establishing a Code for Your SOC. Security Intelligence. Accessed: Feb. 4, 2023. [Online]. Available: https://securityintelligence.com/articles/cybersecurity-ethics-establishing-a-code-of-conduct-for-soc/

[9] D. Kozhuharova, A. Kirov, and Z. Al-Shargabi, ''Ethics in cybersecurity. What are the challenges we need to be aware of and how to handle them?'' in *Cybersecurity of Digital Service Chains* (Lecture Notes in Computer Science), vol. 13300, J. Kołodziej, M. Repetto, and A. Duzha, Eds. Cham, Switzerland: Springer, 2022, doi: 10.1007/978-3-031-04036-8_9.

[10] A. Pawlicka, M. Choraś, M. Pawlicki, and R. Kozik, ''A $10 million question and other cybersecurity-related ethical dilemmas amid the COVID-19 pandemic,'' *Bus. Horizons*, vol. 64, pp. 729–734, Nov. 2021.

[11] C. Véliz, ''Privacy and digital ethics after the pandemic,'' *Nature Electron.*, vol. 4, no. 1, pp. 10–11, Jan. 2021.

[12] A. Pawlicka, M. Choraś, R. Kozik, and M. Pawlicki, ''First broad and systematic horizon scanning campaign and study to detect societal and ethical dilemmas and emerging issues spanning over cybersecurity solutions,'' *Pers. Ubiquitous Comput.*, vol. 27, no. 2, pp. 193–202, Jan. 2021.

[13] K. Delaney. (2014). *A Practical Guide: Introduction to Horizon Scanning in the Public Sector*. Accessed: Feb. 4, 2023. [Online]. Available: https://www.semanticscholar.org/paper/Innovation-toolkit-a-practical-guide%3A-Introduction-Delaney/b6a7d342efdedf4a3901db3a7ddcf0817d60bb49

[14] P. Hines, L. Hiu Yu, R. H. Guy, A. Brand, and M. Papaluca-Amati, ''Scanning the horizon: A systematic literature review of methodologies,'' *BMJ Open*, vol. 9, no. 5, May 2019, Art. no. e026764.

[15] K. E. Cuhls, ''Horizon scanning in foresight—Why horizon scanning is only a part of the game,'' *Futures Foresight Sci.*, vol. 2, no. 1, pp. 1–10, Mar. 2020.

[16] E. Amanatidou, M. Butter, V. Carabias, T. Konnola, M. Leis, O. Saritas, P. Schaper-Rinkel, and V. van Rij, ''On concepts and methods in horizon scanning: Lessons from initiating policy dialogues on emerging issues,'' *Sci. Public Policy*, vol. 39, no. 2, pp. 208–221, Mar. 2012.

[17] *Ethical Issues In E-Commerce: Handling Customer Data*, RSI Security, San Diego, CA, USA, 2020.

[18] A. Pawlicka, D. Jaroszewska-Choras, M. Choras, and M. Pawlicki, ''Guidelines for stego/malware detection tools: Achieving GDPR compliance,'' *IEEE Technol. Soc. Mag.*, vol. 39, no. 4, pp. 60–70, Dec. 2020.

[19] C. Fletcher. (2022). Why the Ethical Use of Data and User Privacy Concerns Matter. VentureBeat. Accessed: Feb. 4, 2023. [Online]. Available: https://venturebeat.com/datadecisionmakers/why-the-ethical-use-of-data-and-user-privacy-concerns-matter/

[20] R. Wang, ''Importance of computer ethics and morality in society,'' in *Proc. Int. Conf. Social Develop. Media Commun.*, vol. 631, 2021, pp. 1–10.

[21] *10 Current and Potential Ethical Crises in the Tech Industry*, Expert Panel®Forbes Councils Member, Forbes, Jersey City, NJ, USA, 2021.

[22] SOC Radar. (2022). Behind the Experts' Perspective: Ethical Issues Behind Cybersecurity. SOC Radar. Accessed: Feb. 4, 2023. [Online]. Available: https://socradar.io/behind-the-experts-perspective-ethical-issues-behind-cybersecurity/

[23] J. Goodchild. (2020). Why Data Ethics is a Growing CISO Priority. DarkReading. Accessed: Feb. 4, 2023. [Online]. Available: https://www.darkreading.com/edge/why-data-ethics-is-a-growing-ciso-priority

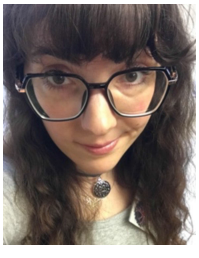
[24] Remoto Workforce Team. (2022). *Roles of a Cyber Security Expert and an Ethical Hacker*. Accessed: Feb. 4, 2023. [Online]. Available: https://www.remotoworkforce.com/roles-of-a-cyber-security-expert-and-an-ethical-hacker/

[25] M. Choraś and M. Woźniak, ''The double-edged sword of AI: Ethical adversarial attacks to counter artificial intelligence for crime,'' *AI Ethics*, vol. 2, no. 4, pp. 631–634, Oct. 2021.

[26] D. Doyle. (2021). Ethical Hacking: What, Why, and Overcoming Concerns. Computer Weekly. Accessed: Feb. 4, 2023. [Online]. Available: https://www.computerweekly.com/opinion/Ethical-hacking-what-why-and-overcoming-concerns

[27] M. Kaufmann, ''The role of ethics in cybersecurity studies,'' Tech. Rep., 2021.

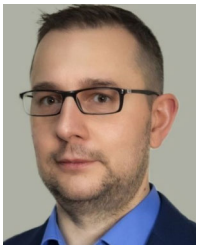
[28] S. Morrow. (2022). Five Ethical Decisions Cybersecurity Pros Face: What Would You Do? InfoSec. Accessed: Feb. 4, 2023. [Online]. Available: https://resources.infosecinstitute.com/topic/five-ethical-decisions-cybersecurity-pros-face-what-would-you-do/
[29] *AI in Cybersecurity: Not an Ethical Dilemma*, Capgemini, Grenoble, France, 2022.
[30] M.-E. Mihailescu, D. Mihai, M. Carabas, M. Komisarek, M. Pawlicki, W. Hołubowicz, and R. Kozik, "The proposition and evaluation of the RoEduNet-SIMARGL2021 network intrusion detection dataset," *Sensors*, vol. 21, no. 13, p. 4319, Jun. 2021.
[31] M. Sweeney. (2022). Ethical Dilemmas in Computer Science. ZDNet. Accessed: Feb. 4, 2023. [Online]. Available: https://www.zdnet.com/education/computers-tech/ethical-dilemmas-computer-science/
[32] F. L. Murtha, P. Jain, and K. Song. (2022). Ethical Issues Surrounding Research of AI in Health Care. Reuters. Accessed: Feb. 4, 2023. [Online]. Available: https://www.reuters.com/legal/litigation/ethical-issues-surrounding-research-ai-health-care-2022-05-31/
[33] M. Choraś, M. Pawlicki, D. Puchalski, and R. Kozik, "Machine learning—The results are not the only thing that matters! What about security, explainability and fairness?" in *Proc. ICCS*, vol. 4, 2020, pp. 615–628.
[34] Teachcyber. (2021). High School Cybersecurity Curriculum Guidelines & Glossary. Teachcyber. Accessed: Feb. 4, 2023. [Online]. Available: https://teachcyber.org/wp-content/uploads/2021/04/High-School-Cybersecurity-Curriculum-Guidelines.pdf
[35] S. Serna. (2021). The Ethical Dilemma Of Paying the Ransomware Crooks. Biznology. Accessed: Feb. 4, 2023. [Online]. Available: https://biznology.com/2021/07/the-ethical-dilemma-of-paying-the-ransomware-crooks/
[36] K. Macaulay and N. Vivion. (2021). Ethics, Privacy and the Creep Factor: The Risk vs. Rewards of the Internet of Behaviors. Catalyst. Accessed: Feb. 4, 2023. [Online]. Available: https://doi.org/https://catalyst.iabc.com/Articles/ethics-privacy-and-the-creep-factor-the-risk-vs-rewards-of-the-internet-of-behaviors
[37] J. Marks. (2021). The Cybersecurity 202: Experts are Split on Whether the Relationship Between Ethical Hackers and Government Has Improved. The Washington Post. Accessed: Feb. 4, 2023. [Online]. Available: https://www.washingtonpost.com/politics/2021/08/04/cybersecurity-202-experts-are-split-whether-relationship-between-ethical-hackers-government-has-improved/
[38] Reciprocity. (2021). The Importance of Ethics in Information Security. Accessed: Feb. 4, 2023. [Online]. Available: https://reciprocity.com/the-importance-of-ethics-in-information-security/
[39] D. Martinis. (2021). 5 Convincing Reasons Teaching CyberEthics is a Must in Today's Environment. Cybercivics. Accessed: Feb. 4, 2023. [Online]. Available: https://www.cybercivics.com/single-post/5-convincing-reasons-teaching-cyberethics-is-a-must-in-today-s-environment
[40] G. Lawton. (2020). 5 Examples of Ethical Issues in Software Development. TechTarget. Accessed: Feb. 4, 2023. [Online]. Available: https://www.techtarget.com/searchsoftwarequality/tip/5-examples-of-ethical-issues-in-software-development
[41] A. Watters. (2021). 5 Ethical Issues in Technology to Watch for in 2021. CompTIA. Accessed: Feb. 4, 2023. [Online]. Available: https://connect.comptia.org/blog/ethical-issues-in-technology
[42] J. Boehm. (2022). Cybersecurity Trends: Looking Over the Horizon. McKinsey. Accessed: Feb. 4, 2023. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon
[43] *A Balancing Act: Privacy, Security and Ethics*, KPMG International, Amstelveen, The Netherlands, 2022.
[44] J. Chukwube. (2021). New Ethical Concerns in Online Privacy and Data Security. Infosecurity Magazine. Accessed: Feb. 4, 2023. [Online]. Available: https://www.infosecurity-magazine.com/next-gen-infosec/ethical-concerns-online-privacy/
[45] M. Hill. (2021). 5 Best Practices for Conducting Ethical and Effective Phishing Tests. CSO. Accessed: Feb. 4, 2023. [Online]. Available: https://www.csoonline.com/article/3619610/best-practices-for-conducting-ethical-and-effective-phishing-tests.html
[46] K. A. Muñoz, K. Kostick, C. Sanchez, L. Kalwani, L. Torgerson, R. Hsu, D. Sierra-Mercado, J. O. Robinson, S. Outram, B. A. Koenig, S. Pereira, A. McGuire, P. Zuk, and G. Lázaro-Muñoz, "Researcher perspectives on ethical considerations in adaptive deep brain stimulation trials," *Frontiers Hum. Neurosci.*, vol. 14, 2020, doi: 10.3389/fnhum.2020.578695.
[47] S. Buchholz and B. Ammanath, "Quantum computing may create ethical risks for businesses. It's time to prepare," Tech. Rep., 2022.
[48] I. Tuisawau. (2021). Opinion/From the Crowd Facebook Exposed—Cybersecurity Ethical Issues. The Fiji Times. Accessed: Feb. 4, 2023. [Online]. Available: https://www.fijitimes.com/facebook-exposed-cybersecurity-ethical-issues/
[49] A. Farnell. (2022). Should I Be Worried About Where My Cybersecurity Students Will End Up? Times Higher Education. Accessed: Feb. 4, 2023. [Online]. Available: https://www.timeshighereducation.com/opinion/should-i-be-worried-about-where-my-cybersecurity-students-will-end
[50] C. A. Makridis and J. Thacker. (2020). Cybersecurity is a Moral Necessity. Providence. Accessed: Feb. 4, 2023. [Online]. Available: https://providencemag.com/2020/08/cybersecurity-moral-necessity-big-tech/
[51] J. Meyers. (2020). Best Practices for Ethically Teaching Cybersecurity Skills. TechTarget. Accessed: Feb. 4, 2023. [Online]. Available: https://www.techtarget.com/searchsecurity/post/Best-practices-for-ethically-teaching-cybersecurity-skills
[52] Navigate Human Resources Consultants. (2021). *Cyber Security and Ethics*. Accessed: Feb. 4, 2023. [Online]. Available: https://www.navigatehr.in/cyber-security-and-ethics.html
[53] L. Irwin. (2021). Ethical Hacking vs Penetration Testing: What's the Difference? IT Governance. Accessed: Feb. 4, 2023. [Online]. Available: https://www.itgovernance.eu/blog/en/ethical-hacking-vs-penetration-testing-whats-the-difference
[54] K. Price, M. Schreiber, and S. Ferber. (2022). Cybersecurity Whistleblowers are Different. Here's How to Deal With Them. Corporate Compliance Insights. Accessed: Feb. 4, 2023. [Online]. Available: https://www.corporatecomplianceinsights.com/emerging-cyber-whistleblower/
[55] K. R. Gangarapu. (2022). Ethics of Facial Recognition: Key Issues and Solutions. Learn.G2. Accessed: Feb. 4, 2023. [Online]. Available: https://learn.g2.com/ethics-of-facial-recognition
[56] P. Pavlova, "Human rights-based approach to cybersecurity: Addressing the security risks of targeted groups," *Peace Hum. Rights Governance*, vol. 4, no. 3, pp. 391–418, 2020.
[57] T. Madsen. (2022). Ethics of the 0-Day Trade. CyberSecurity Magazine. Accessed: Feb. 4, 2023. [Online]. Available: https://cybersecurity-magazine.com/ethics-of-the-0-day-trade/
[58] Z. Sterling. (2021). Data as an Object of Ethical Concern. Zoughts. Accessed: Feb. 4, 2023. [Online]. Available: https://zoughts.medium.com/data-as-an-object-of-ethical-concern-5eca3f5e7aea
[59] F. Tronnier, S. Pape, S. Löbner, and K. Rannenberg, "A discussion on ethical cybersecurity issues in digital service chains," in *Cybersecurity of Digital Service Chains* (Lecture Notes in Computer Science), vol. 13300, J. Kołodziej, M. Repetto, and A. Duzha, Eds. Cham, Switzerland: Springer, 2022, doi: 10.1007/978-3-031-04036-8_10.
[60] M. Jeyaretnam. (2022). Yale Cyber Leadership Forum Hosts Discussion on 'AI Ethics and Safety'. Yale News. Accessed: Feb. 4, 2023. [Online]. Available: https://yaledailynews.com/blog/2022/04/04/yale-cyber-leadership-forum-hosts-discussion-on-ai-ethics-and-safety/
[61] A. Kaspersen and W. Wallach. (2022). We're Failing at the Ethics of AI. Here's How We Make Real Impact. World Economic Forum. Accessed: Feb. 4, 2023. [Online]. Available: https://www.weforum.org/agenda/2022/01/we-re-failing-at-the-ethics-of-ai-here-s-why/



ALEKSANDRA PAWLICKA received the Ph.D. degree. She is a philologist and a research and development specialist. She is the author of a number of multidisciplinary scientific publications, and has been involved in several international projects, such as H2020 SIMARGL, H2020 SPARTA, and H2020 PREVISION. Her research interests include computer science, linguistics, language teaching and learning, and pedagogy.

MAREK PAWLICKI received the Ph.D. (Eng.) degree. He currently holds an adjunct position with the Bydgoszcz University of Science and Technology. He has been involved in a number of international projects related to cybersecurity, critical infrastructures protection, and software quality (e.g., H2020 SPARTA, H2020 SIMARGL, H2020 PREVISION, H2020 MAGNETO, H2020 Q-Rapids, and H2020 SocialTruth). He is the author of over 60 peer-reviewed scientific publications. His research interest includes the application of machine learning in several domains, including cybersecurity.

RAFAŁ KOZIK received the Ph.D. degree in telecommunications from the University of Science and Technology (UTP), Bydgoszcz, in 2013, and the Doctor of Science (D.Sc.Eng.) degree in computer science from the West Pomeranian University of Technology, Szczecin, in 2019. He is currently a Professor with the Bydgoszcz University of Science and Technology, Bydgoszcz. Since 2009, he has been involved in a number of international and national research projects related to cybersecurity, critical infrastructures protection, software quality, and data privacy (e.g., FP7 INTERSECTION, FP7 INSPIRE, FP7 CAMINO, FP7 CIPRNet, SOPAS, SECOR, and H2020 Q-Rapids). He is the author of over 140 reviewed scientific publications.



MICHAŁ CHORAŚ is currently a Full Professor with the Bydgoszcz University of Science and Technology, Bydgoszcz, where he is also the Head of the Teleinformatics Systems Division and the PATRAS Research Group. He is also affiliated with FernUniversität Hagen, Germany, where he was a Project Coordinator for H2020 SIMARGL: Secure Intelligent Methods for Advanced RecoGnition of malware and stegomalware. He is the author of over 280 reviewed scientific publications. His research interests include data science, AI, and pattern recognition in several domains, e.g., cyber security, image processing, software engineering, prediction, anomaly detection, correlation, biometrics, and critical infrastructures protection. He has been involved in many EU projects (e.g., SocialTruth, CIPRNet, Q-Rapids, and InfraStress).