Short Paper: Debating Ethics *with* Cybersecurity Students

Jan Breig[1] Dirk Westhoff[2]

Abstract: We aim to debate and eventually be able to carefully judge how realistic the following statement of a young computer scientist is: "*I would like to become an ethical correctly acting offensive cybersecurity expert*". The objective of this article is not to judge what is good and what is wrong behavior nor to present an overall solution to ethical dilemmas. Instead, the goal is to become aware of the various personal moral dilemmas a security expert may face during his work life. For this, a total of 14 cybersecurity students from HS Offenburg were asked to evaluate several case studies according to different ethical frameworks. The results and particularities are discussed, considering different ethical frameworks. We emphasize, that different ethical frameworks can lead to different preferred actions and that the moral understanding of the frameworks may differ even from student to student.

Keywords: Cybersecurity; ethical frameworks; offensive security techniques

1 Introduction

From our viewpoint it is essential for the well-being of a modern digitized society to educate people with a strong knowledge not only in computer science, but in particular in IT-security respectively cybersecurity. Over the recent years, a plethora of new job descriptions have emerged in this field, e. g. malware analyst, threat hunter, threat intelligence analyst, pentester etc.. This also includes to some degree offensive techniques, aiming to successfully attack systems. However, it is of similar or even more importance that these people also possess a strong moral compass. Just because a security expert has the capability to exploit security vulnerabilities, it is highly desirable that he/she can discipline himself/herself not to perform such actions in the wild. On the other hand, companies, authorities and countries require persons with such technical IT-capabilities to better understand how to defend their systems, economy and society from massively increasing number of attacks via the Internet.
To debate this and to build up a common understanding is not only beneficial for the individual security expert himself, but also for the society. Use cases have been offered for debating ethical questions according to the daily work of the general computer science community [GI]. In this article, we would like to debate more specific ethical questions for the increasing and demanding subgroup of cybersecurity experts. Recently Macnish and van der Ham have identified the missing of a proper ethical education at an undergraduate and postgraduate level [Mv20] for computer scientists. They recommend that ethics should be taught in far greater depth on computer science courses than it is currently the case.

[1] Hochschule Offenburg, Badstraße 24, 77652 Offenburg, Germany jan.breig@hs-offenburg.de
[2] Hochschule Offenburg, Badstraße 24, 77652 Offenburg, Germany dirk.westhoff@hs-offenburg.de

doi:10.18420/sicherheit2022_12

Moreover, they point out that typically Research Ethics Boards (REB) fail to propose reasonable ethical proposals for cybersecurity experts due to the lack of their own expertise. Exactly this is the strength of the work at hand since it involves upcoming cybersecurity experts in the judgment of various case studies after they attended the ethics lecture at HS Offenburg.
Let us for the moment forget that by pointing out that such a concrete and specific professional wish "*I would like to become an ethical correctly acting offensive cybersecurity expert*" is rather seldomly the case. However if it turns out, that on the one side the wish to always act ethically correct and on the other side the profession to be an offensive cybersecurity expert is an unsolvable dilemma, does this mean that the society ends up in a situation that most human beings which would like to act ethically correct will decide to not become a cybersecurity expert? Moreover, would this also mean that an over-proportional number of actually active offensive cybersecurity experts does not really care about moral or ethical acting since those who are aware of this dilemma have not started such a carrier in the first place or did just quit the job? Where exactly is the borderline of techniques and toolsets to be used between a cybersecurity expert and an offensively acting cybersecurity expert e. g. what about port scanning and other elementary techniques to spy out a victim to prepare an active attack? Can an *arp -a* or a *ping* yet be considered as belonging to the first phase of a cyber-kill-chain [Lo]? Is it sufficient to argue that *white hat hackers* have their own code of ethics e. g. ground rules are established with the defender regarding targets and in what is off-limits and that *certified ethical hackers* always have undergone a rigorous moral and law inspection? Does this end the overall discussion? Obviously, we cannot answer all these questions within such an article. However, we would like to open the discussion with respect to a *correct ethical acting or at least reflected ethical acting for offensive cybersecurity experts*.

2 Philosophical Ethical Frameworks

Over the centuries, the philosophical prophets of their epoch established several directions like *Virtue Ethics* (Aristoteles (384-322 B. C.)), *Ethics of duty* (Immanuel Kant (1724-1804)), *Utilitarianism* (John Stuart Mill (1806-1873)), *Ethics of responsibility* (Max Weber (1864-1920)) or *Ethos ethics* (Albert Schweitzer (1875-1965)) to name a few. Will the fundamental rules of what acting is considered to be good or evil, right or wrong, or virtue and vice argued in some of these ethical frameworks indeed support the insights of our offensive cybersecurity expert 'in spe' even if these ethical frameworks definitively could not have considered dilemmas that arose due to the appearance of the cyberspace?
According to three predominant different philosophical ethical frameworks, Virtue, Utilitarian and Deontological Ethics, a human being, in our case a cybersecurity expert [Ma18, p.49], may like to ask the following questions to decide what is ethically justifiably:

Virtue Ethics (VE): Which position best expresses my value and character? If I choose this, can I live with myself?

Utilitarian Ethics (UE): Which position will give the greatest positive utility and produce the fewest negative consequences? What costs respectively benefits are associated with each outcome?
Deontological (DE): Who will be affected by this decision? Am I treating others as a means or an end in themselves? If my actions became a rule and I myself was subject to that rule, would I accept it and view it as ethical?

In [Ma18, p.49] Manjikian summarizes the pros and cons for the usage of such philosophical frameworks in today's decision processes. Here we aggregate some of them: The strong point of Aristotle's Virtue Ethics approach is, that it creates consistent ethical positions across issues and it emphasizes the character of decision making. As a downside Manjikian argues, that the framework is traditional and therefore perhaps outdated in new environments. The calculations of the utilitarian ethics approach are "clean and often value free". It is universally valid and not based on the value of a particular culture. As a clear downside, the approach expects to adopting an instrumental view of human beings as means to an end. Human being own rights are fully ignored. Kant's deontological approach is judged by Manjikian such that the focus is on those affected by decisions. Its clear benefit is the reciprocal character forcing the acting party to see himself as both decider and subject of decision. As the downside with Kant's approach, she argues that it "overemphasizes duty to individuals over duty to produce the best possible outcome".

3 Acting in Contexts - Professional Life

Moreover, our security expert 'in spe' may also come to a point where he/she asks himself/herself whether it is morally justifiably to ethically act and behave differently in different contexts e. g. at home, in the public space, as an online user and, finally, as a professional actor. For the latter, does it make a difference to ask: "How should I act ethically as an employee? ...as a computer scientist? ...as cybersecurity expert? ... as an offensive cybersecurity expert?" With respect to an ethically correct behavior does it make a difference for an offensive cybersecurity expert who will be the employer. Eventually a security expert will receive job offers from companies, governmental and/or intelligence agencies, public authorities or the military.
Here, belonging to one or another employer does surely make a difference. Similar can be stated with respect to the concrete circumstances which in some cases might even allow for public authorities to use tools like e. g. *Staatstrojaner* or *Pegasus*. Sometimes, acting in conformity to law may still be unethical. Obviously, the opposite can also be the case ending for some people in a personal moral dilemma which frequently cannot be resolved over the long run.[3] Of course there are also many situations which are solvable without moral dilemma e. g. pentests carried out with previous agreement or situations where many if not all individuals would agree that a certain behavior is ethically un/justifiable.[4]

[3] Note that in this article we are not debating if a person is acting in conformity to law.
[4] However since the goal is to become aware of and discuss potential moral dilemmas, these situations are not taken into account in this article.

4 Ethical Frameworks for Cyber-communities

Moreover, we can observe that shortly after the appearance of the Internet era more specific ethical frameworks were either implicitly or explicitly established [Ma18, p.63].

Old Hacker Ethic: "Information wants to be free", laws do not apply in cyberspace, transparency is more important than privacy.
New Hacker Ethic: Community should govern itself, privacy is important, don't freeload.
Professional Hacker Ethic: Professional organization sets behavior norms, theft of personal information is not ethically justifiable, nations can regulate cyberspace.

We can also mention the work of *Research Ethic Boards* who are installed to judge the activities within various research directions in academia. However, as pointed out in [Mv20], the members of such boards rarely have the competence or technical background to judge cybersecurity related questions. The GI's ethical guidelines for computer scientists, encouraging people to critical thinking, also rarely help when it comes to the sometimes very specific situations a cybersecurity expert may face during his work. Due to this, we consired the outcome of our discussions about ethics *with* cybersecurity students to be of interest for the overall IT-security community. .[5]

5 Individual's Moral Compass and Community's Code of Conduct

The moral compass in philosophical ethics, recommending concepts of right and wrong conduct is indeed envisioned to be a fundamental part of each individual human being. But also groups, communities or the society as a whole may either implicitly or explicitly follow an ethical framework or (at least) a code of conduct as another agreed norm of right behavior besides the pure law. The fundamental problems applied ethics has to deal with has been verbally illustrated by the trolley problem [Fo78] in which a person must decide between killing one person or letting several persons die. What should be emphasized is that the trolley problem points out a decisional dilemma thus, the recommendation of right and wrong conduct is not always such clear. We can also observe from the trolley problem, that in some cases simply not acting does mean having chosen implicitly and thus also having to life with the consequences.
Independently of any companies', government agencies', or even intelligence agencies' written or silently agreed code of conduct, *whistleblowing* may frequently start with an ethical dilemma, where a human being belonging to a group or community recognizes a conflict of his own values with the values of the unit he is working for. Or, speaking in the notion of the trolley problem: The employee values the survival of multiple persons higher than the survival of one person (or vice versa). Since both sides, the whistleblower as well as the group/community, may act ethically correct within 'their' chosen ethical frameworks, we observe that indeed, in specific situations, different ethical frameworks may contradict in what is considered to be good and wrong respectively.

[5] In contrast to discuss ethics *for* cybersecurity experts without considering their view.

6 Applying Ethical Frameworks

Next we describe three exemplary case studies along the supply-chain of vulnerabilities and exploits of IT-ecosystems. We will see, that some of these case studies do not necessarily involve a cybersecurity expert. However even here either a significant amount of personal data is leaked, or later exploitation would not be possible without a previous situation like this. So when we talk about ethical behavior along the supply-chain of vulnerabilities and exploits of IT-ecosystems, ethical behavior is not only required by cybersecurity experts. Instead, when we want to mitigate security vulnerabilities we also have to talk about morally sound behavior of other actors.
The tables within the following subsections have been anonymously filled out by 14 international students of a cybersecurity master program when attending the ethics seminar. These students are ideal to be interviewed for such a little study since they are yet on their career path to become a cybersecurity expert. Obviously such a small data set is not representative. Nevertheless, it may serve to better understand arising personal dilemma of cybersecurity experts. Students have first been requested to i) fill out what *they believe* would be the outcome from the application of the three philosophical ethical frameworks to various cybersecurity related case studies (VE, UE, DE). Secondly, ii) they should judge what *they believe* would be the outcome when applying different ethical frameworks for cyber-communities. Finally, iii) they should provide *their own personal judgment*.[6]
The notation **+x**, **−x** and **0x** in tabulars 1, 2 and 3 means, that **x** students believe the concrete action is justifiable, unjustifiable or undecidable respectively within the given ethical framework. We aggregated the outcome by purely listing the majority of all votes (out of 14 possible votes). Thus a value of +10 (ten students voted justifiable) also means that four students either voted **0** (unjustifiable) or **–** (undecidable).

6.1 Case study 1: App development

Before we start debating ethical dilemmas cybersecurity experts may face, let us for the moment consider the work of an App programmer. This person would never claim to be an offensive security expert, since his knowledge is limited to Java programming, in particular the development of mobile Apps.

Careless App-Developer: May tend to implement the app asking for more permissions such that at the end the running software is over-privileged e. g. to assure that the internet connection is not blocked by too strict access rights.

Intentional App-Developer: Is aware that due to the old/new Android permission system the App can perform silently by far more actions than the user of the App becomes aware of [Er21]. Although his App is promoted to only provide service X, he has implemented more and more functionalities (internet connection, camera, SMS, phone, BT). At some

[6] One of the students did not fill out the category personal judgment.

point in time he decided to obfuscate the code such that it passes the static/dynamic code analysis check to be available in the App store just due to curiosity. In particular he obfuscated the internet connection transmitting the harvested personal data to a server with a concrete IP-address. However, at some point in time he decides to provide his App 'Give me everything' (of course he gave it another name say X) to the Appstore. Luckily, the app passes the security checks and thus is available in the store. Meanwhile it has been downloaded and used more than 100.000 times worldwide which means that the storage capacity of his servers are definitely too small. Maybe he should reconsider selling his App to a company that is more powerful and which could set up a suitable storage-system in the back-end for such an amount of user data. The students' answers for this use case are aggregated in tabular 1 according to the notation introduced in section 6.

	VE	**UE**	**DE**	**Old Hacker Ethic**	**New Hacker Ethic**	**Prof. Hacker Ethic**	**Personal Judgment**
Provide service X	+11	+12	+10	+11	+12	+11	+10
Additional functionality	+7	+10	–6	+12	+10	+8	–8
Obfuscation	–10	–7	–13	+11	–10	–12	–11
Send data to company	–10	+8	–12	+10	–11	–12	–10

Tab. 1: Students moral understanding according to different ethical frameworks and own personal judgment for case study on careless/intentional mobile App development.

6.2 Case study 2: Storage corruption vulnerabilities

The next person would definitively claim himself as cybersecurity expert. He build-up significant knowledge with respect to the Windows Memory protection means like Safe CRT, GS-Cookies, ASLR/DEP, Safe-SHE) and how to circumvent them. Naturally such knowledge is extremely valuable for a number of actors in the field of IT-security. In parallel to his bachelor studies he educated himself with respect to classical storage corruption vulnerabilities (StoCV) and early mitigation techniques, first by reading articles and blogs with respect to this issue and subsequently by building a PoC to demonstrate the attack for older Windows operating systems. However, he was also interested why for actual Windows versions such PoCs are not successful anymore. Thus, he also studied the details of actual in use storage-corruptions means in depth which mitigate the vulnerability of storage-corruption. During this study – in the spare-time to his bachelor studies – he got an idea how to corrupt also the storage of current operating system versions. To check whether his idea indeed succeeds, he built a PoC also here and yes it works! Up to this moment he had never the intention to make use of his knowledge. However, due to an unforeseeable and unpleasant personal economic situation – due to the COVID pandemic situation he lost his job in a restaurant – he considered to anonymously sell the PoC. Since he never used his PoC to attack a concrete person, nor does he know if the party which he sold the PoC is actually using it, respectively for which concrete destinations it will be used, he judged his

decision to be morally justifiable. The students' answers for this use case are aggregated in tabular 2.

	VE	UE	DE	Old Hacker Ethic	New Hacker Ethic	Prof. Hacker Ethic	Personal Judgment
Build up StoCV knowledge	+8	+12	+9	+10	+12	+11	+10
PoC for classical StoCV	+9	+13	+11	+10	+12	+10	+9
Get familiar with protection	+11	+10	+10	+11	+13	+10	+11
PoC to bypass protection	+9	+7	+9	+10	+10	–8	–6
Anonymously sell the PoC	–9	–7	–11	–7	–7	–10	–12

Tab. 2: Students moral understanding according to different ethical frameworks and own personal judgment for case study on storage corruption vulnerabilities.

6.3 Case study 3: Cyber-Kill-Chain

Offensive cybersecurity experts are required to be experienced in attacking systems, spying out individuals, installing malware, controlling victims remotely etc.. Lockheed Martin [Lo] developed the cyber-kill-chain with the objective to structure such a process and address advanced persistent threats (APT). The five phases of the cyber-kill-chain according to [Lo] are: 1. Reconnaissance (harvesting email addresses, conference information), 2. Weaponization (coupling exploit with backdoor into deliverable payload), 3. Delivery (deliver weaponized bundle to the victim via email, web, USB, etc.), 4. Exploitation (exploiting a vulnerability to execute code on victim's system) and 5. Actions on Objective (accomplishing original goals with 'hands on keyboard'). The students' answers for this use case are aggregated in tabular 3.

	VE	UE	DE	Old Hacker Ethic	New Hacker Ethic	Prof. Hacker Ethic	Personal Judgment
Reconnaissance	–8	+10	–8	+10	+8	–9	–6
Weaponization	–9	+7	–12	+9	+8	–11	–8
Delivery	–9	+7	–11	+9	–7	–10	–11
Exploitation	–10	+8	–12	+9	–7	–10	–11
Installation	–9	+7	–10	+9	–8	–10	–11
Command and Control	–11	–8	–12	+9	–7	–10	–11
Actions on Objective	–10	+8	–12	+9	+7	–10	–11

Tab. 3: Students moral understanding according to different ethical frameworks and own personal judgment for case study on cyber-kill-chain.

6.4 Remarks on Case Studies

As yet said, with such a small data set the results are not representative. Any form of statement made here can therefore not be generalized. Nevertheless, we want to share some of our observations. Not surprisingly, there is a tremendous difference what students believe what actions are ethical and unethically with respect to the different ethical frameworks. This holds for all debated case studies. The students' personal judgment matched different ethical frameworks for the different case studies.[7] Recall that with respect to their personal judgment the students did not explicitly follow a specific ethical framework, instead they decided rather intuitively. Generally, they were also quite restrictive in evaluating actions as ethically justifiable.

Remark 1: In particular phase 1 of the cyber-kill-chain seems to be debatable. Everyone would agree, that normally searching for someone's e-mail address over the public Internet is by far not an unethical act. However, if this yet is done with the intention to later attack this person, even phase 1 can be considered as highly unethical according to the classical ethical frameworks VE and DE.

Remark 2: It is frequently the case that those parties attacking a victim according to the various steps listed in the cyber-kill-chain do not implement exploits with respect to specific vulnerabilities on their own. Instead they buy such exploits from security companies or individuals which sell them over some platforms. How can the behavior of those security experts be judged that do on the one side implement the exploits, do never perform the cyber-kill-chain with respect to a concrete victim on their own, but (anonymously) sell it to actors which from that point on can and will apply the cyber-kill-chain to potentially every possible victim. Is the argumentation of those persons justifiable, who argue, since they do neither know the victim nor perform the concrete attack they do not act unethically?

Remark 3: In particular with respect to the case study three we expected some hints regarding the whistleblower's dilemma[8]: In particular the hacker ethics have been elaborated from communities and have also been adapted to the needs of these communities. Naturally, there should be significant conflicts with the moral compass of the classical ethical frameworks, otherwise, we assumed, there would not have been the need to establish them. However, amazingly at least from the students' votes we could not validate this. The judgments for VE, DE as well as the professional hacker ethics are almost equivalent.

Remark 4: Over all case studies, the old hacker ethic as well as UE evaluate most actions as ethical. The evaluations for VE, DE, new and professional hacker ethic were also rather similar. It turns out, that overall the traditional ethical framework UE has a better mapping to the old hacker ethic than with other traditional frameworks.

[7] Ethical frameworks with similar evaluation are marked with gray color in the tables.
[8] In 2019 the European Institution has presented a common statement for a whistleblowing guideline.

Remark 5: An individual, over the long run, may, either intuitively or reflected, orientate his/her own moral compass more with respect to one of the classical philosophical ethical frameworks. When the orientation is in line with VE, we expected that this may almost certainly result in a personal dilemma and conflict for the employee. The situation is getting even more problematic if he/she has to switch from one ethical framework to another one according to the various contexts he/she currently is involved in (private, public, professional). In particular following the framework of virtue ethics does not allow dividing one's actions e. g. public life, private life and professional life. We expected that, if the employee in the field of cybersecurity is dedicated to professional hacker ethic, the personal moral dilemma of such person is almost foreseeable. As said, the students' output does not justify this. Instead, VE and professional hacker ethic are evaluated similarly by them.

7 Discussion

The society as a whole should have an increasing interest, that in particular young people with a strong moral compass will choose a cybersecurity career. Citizens, companies, towns, regions and countries are increasingly dependent from digital processes and critical infrastructures. To secure and defend such infrastructures it is essential to understand how concrete attacks are performed. Thus, a security expert always needs to be educated also in offensive security means. With this powerful knowledge it is almost self-explanatory that such people have to be educated such that they are able to build up a sustainable strong moral compass. Such strong characters are essential for almost every level of a hierarchy within a team acting in the area of cybersecurity and should thus be carefully balanced with respect to the overall demand for loyalty within the group. This is obviously predominant for positions in authorities, military, but also 'common' cybersecurity companies, since the latter frequently equip the aforementioned with technology (See remark 2). A first, however indeed very small step towards this direction, is to educate these people in cybersecurity ethics and pinpoint to the dilemma of controversial ethical frameworks. However, much more activities are surely required here. Applying the various ethical frameworks results in different recommendations how to morally act with respect to concrete cybersecurity case study steps. This was an outcome of our small cybersecurity study with international students. We assume that this may sometimes result in ethical trade-offs of employee vs. employer. Consequently, a good balance of tolerating different ethical cybersecurity viewpoint versus loyalty within the cybersecurity team may be required here. Our assumption is that cybersecurity related companies and authorities tend more to be in line with community driven ethical frameworks like professional hacker ethic, human being decisions however over the long run may tend to be VE, or DE dominated. We also observe that the vulnerability and exploit supply-chain is never purely influenced by cybersecurity actors. Also, careless developers and users have a significant portion here. Moreover, one proposal we could make is that also cyber-experts who are in particular oriented towards a VE or DE driven ethical framework *have to* become part of a security team since we believe that a good mix is required to provide better results and acceptability for overall society. An open issue is how to ethical act as a cybersecurity

expert with respect to real-time challenges (e. g. trolley problem) where different acting options due to different ethical frameworks cannot be debated since one has to decide and act immediately. This observation encourages our believe that teams of people with mixed ethical background are in particular good when formulating the code-of-conduct of a team. However, the more it comes to real-time responsive decision making, the less time is available to find a consensus between different and maybe contradicting ethical frameworks of the group.

8 Conclusion

We discussed potential ethical dilemma security experts may face during their professional career. Although we could not provide the solution how to resolve such dilemma, we feel it is yet an important step forward to transparently discuss these issues. This is why we decided to publish an aggregated summation of the debates with young upcoming cybersecurity experts within our ethics seminar to share with a broader audience. We conclude with an enhanced and more mature statement: "*I would like to become an ethical dilemma aware offensive cybersecurity expert*".

9 Acknowledgments

We want to thank the anonymous reviewers, in particular our shepard Bernhard Hämmerli.

References

[Er21] Erden, Ç.: Give Me Everything: Analyzing leakage of information in the Android platform with respect to wireless communication and personally identifiably information, MA thesis, Hochschule Offenburg, Aug. 2021.

[Fo78] Foot, P.: Virtues and Vices and Other Essays in Moral Philosophy. Clarendon Press, Oxford, 1978.

[GI] GI-Fachgruppe Informatik und Ethik: Gewissensbits, Fallbeispiele zu Informatik und Ethik, URL: https://gewissensbits.gi.de/, visited on: 09/09/2021.

[Lo] Lockheed Martin Rotary and Mission Systems: Cyber Kill Chain, URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html, visited on: 09/15/2021.

[Ma18] Manjikian, M.: Cybersecurity ethics: an introduction. Routledge, 2018.

[Mv20] Macnish, K.; van der Ham, J.: Ethics in cybersecurity research and practice. Technology in Society 63/C, 2020.