Cybersecurity and the Ethics of Care

Jane Blanken-Webb
Wilkes University, University in Wilkes-Barre
Pennsylvania, USA

Ryan Cloutier
Security Studio
Greater Minneapolis
USA

ABSTRACT: *This paper addresses mounting calls for ethical inquiry in cybersecurity by proposing consideration of the ethics of care as a guiding philosophical framework. It offers a general introduction to the ethics of care in relation to cybersecurity, followed by a targeted discussion of care ethics' unique contribution as a philosophical framework for considering cybersecurity's position at the edge of technological innovation. From there, the paper puts forth a first-hand example, based on the second author's personal experience as a cybersecurity professional, demonstrating a lived experience of the ethic of care in the midst of professional practice in cybersecurity. This opens into broader consideration of a fundamental ethical paradox in cybersecurity, discussed through the lens of the ethics of care, followed by discussion of the significance of the relational context—or ethos—that surrounds ethical action in cybersecurity education and practice. In closing, the paper proposes that the field of cybersecurity is inherently linked with care.*

Keywords: Cybersecurity Ethics, Ethics of Care, Philosophical Foundations of Cybersecurity Ethics

Received: 27 December 2020, Revised 23 January 2021, Accepted 14 February 2021

DOI: 10.6025/isej/2020/7/2/31-39

1. Introduction

Situated at the intersection of technological advancement and today's global society, cybersecurity pushes the boundaries of what is possible at the same time that it touches ever-more-deeply into the intimate details of billions of people's lives all around the planet. From the Stuxnet computer worm that was the first to cross the cyber-physical barrier (Langer, 2011) to the presence of highly detailed profiles of human health, education, genetics, environmental, and lifestyle factors (Azmak et al., 2015), cybersecurity rests at the precipice of new possibilities that pose significant ethical challenges. Yet, as it stands, there is no commonly accepted ethical framework for beginning to approach cybersecurity, let alone codified standards of ethics that adhere for the field (Macnish & van der Ham, 2020; Ramirez et al., 2020; Shoemaker et al., 2019; Bradbury, 2016; Kenneally & Bailey, 2014).

Our aim in this paper is to address mounting calls for ethical inquiry in cybersecurity by proposing consideration of the ethics of care as a guiding philosophical framework. We begin with a brief overview of available literature pertaining to the foundations of cybersecurity ethics. Next, we offer a general introduction to the ethics of care in relation to cybersecurity, followed by a more targeted discussion of care ethics' unique contribution as a philosophical framework for considering

cybersecurity's position at the edge of technological innovation. From there, we put forth a first-hand example, based on the second author's personal experience as a cybersecurity professional, demonstrating a lived experience of the ethic of care in the midst of professional practice in cybersecurity. This opens into broader consideration of a fundamental ethical paradox in cybersecurity, discussed through the lens of the ethics of care, followed by discussion of the significance of the relational context—or ethos—that surrounds ethical action in cybersecurity education and practice. In closing, we propose that the field of cybersecurity itself is inherently linked with care.

2. Foundations of Cybersecurity Ethics

Amid mounting calls for ethical inquiry in cybersecurity (Macnish & van der Ham, 2020; Webb, 2019; Knowles, 2016; Bradbury, 2016; Leonhard, 2016), available literature often focuses on applied issues such as privacy (Davis et al., 2018), machine learning (Miller, 2019), internal cyber-stings (Luck, 2019), or cyber war (Dipert, 2010). Automated ethical support tools have also been recently proposed based on models of human ethical decision making (Ramirez et al., 2020; Hoppa, 2018).

In contrast with these approaches, the contribution proposed in this paper speaks to the philosophical foundations of cybersecurity ethics, an area of inquiry with a distinct disciplinary focus that is still only beginning to take shape. A general introduction to cybersecurity ethics can be found in Blanken-Webb et al. (2019), which traces the intellectual history of cybersecurity ethics along three distinct lineages: the hacker ethic, cybersecurity professional practice, and philosophical inquiry related to computer and information ethics. The recently published edited volume, *The Ethics of Cybersecurity* (Christen et al., 2020) offers in depth consideration of cybersecurity ethics, organized in terms of foundations, problems, and recommendations. Included in this volume is a chapter by Loi and Christen (2020), which addresses ethical frameworks for cybersecurity that emphasize principle-based and human rights-based approaches that have emerged from within the field of cybersecurity. The authors ultimately conclude that an ethics of risk pose a necessary complement to considerations of cybersecurity ethics and draw upon Nissenbaum's contextual integrity theory to guide understandings of expectations of human interactions with cybersecurity practices (Christen & Loi, 2020). Another recent contribution is a textbook, entitled *Cybersecurity Ethics* by Manjikian (2018), which briefly mentions a variety of ethical frameworks, followed by extended consideration of deontological ethics, utilitarian ethics, and virtue ethics—the three most common frameworks within the Western philosophical tradition.

Previous analyses that utilize the ethic of care have also been put forth in relation to cybersecurity ethics. In particular, Morgan and Gordijn (2020) consider how best to respond to ransomware in the business context, utilizing care theory in connection with stakeholder theory. Additionally, Friedman's (2015) philosophical analysis of privacy and security engages established connections between the ethics of care and security as well as consideration of privacy through the perspective of care. Ultimately, Friedman (2015) argues for an approach that balances issues of security and privacy through the lens of care ethics.

Rather than focusing on specific ethical problems in cybersecurity and offering analyses through the lens of care ethics, our aim in this paper is more overarching, aspiring to demonstrate that the ethics of care forwards a philosophical perspective that is worthy of being taken seriously for advancing ethical inquiry in cybersecurity. Accordingly, our proposed contribution is very much in line with Nair and Bulleit's (2020) recent article that describes how philosophical pragmatism and the ethic of care stand to provide a fruitful framework for approaching engineering ethics. Indeed, drawing on Nair's earlier work, the emphasis on care ethics we propose herein is a direct extension of the observation that "engineering, like care, emerges as a response to a need and is oriented towards practice" (Pantazidou & Nair, 1999, p. 211). The discussion continues below with a general introduction to the ethics of care.

3. The Ethics of Care

The ethics of care (also referred to as care ethics) forwards a distinctly contextual logic that incorporates emotion, body, and relationship. In this, the ethics of care transcends beyond long established dualisms (such as mind vs. body, good vs. evil, or selfishness vs. selflessness) that ground many moral theories in their aspiration to achieve objectivity through detachment. Instead, the ethics of care call forth what Carol Gilligan (1993) referred to as *a different voice*. Although care ethics represent a feminist philosophical perspective, this different voice is not inherently male or female; rather, it is a quintessentially human voice that is shockingly absent from many considerations of moral philosophy, but also much of everyday human

living. In her recent work, Gilligan explains that this voice is "different because it joins self with relationships, thoughts with emotions, the mind with the body" (Gilligan & Snider, 2018, p. 107).

Above all, the ethics of care shines a spotlight on the notion that "moral problems are problems of human relations" (Gilligan, 1993, p. xix). This is an interesting insight to consider in conjunction with cybersecurity ethics because it calls us to acknowledge cyber space as an extension of our humanity. Indeed, it is hard to deny that this is the case, especially in light of the connections in cyber space that currently hold together families, friends, and colleagues alike, when they must be physically apart during the ongoing COVID-19 pandemic.

Yet, while cyber space can, indeed, meaningfully be understood as an extension of our humanity, it is an *extension* nonetheless. Hence, there is at least some degree of distance inherent in the care cybersecurity affords. While this may stand at odds with the hands-on, person-to-person caring that lies at the heart of care theory, as conveyed in Noddings' (2013) account of caring-*for*, this is not to diminish care theory's applicability to cybersecurity. Instead, it more precisely locates the kind of caring that best applies to cybersecurity; namely, caring-*about*. This secondary kind of caring is instrumental in that caring-about establishes, maintains, and enhances "the conditions under which caring-for can flourish" (Noddings, 2002, p. 23).

To illustrate this connection with cybersecurity, consider the classic CIA triad of confidentiality, integrity, and availability (Samonas & Coss, 2014). In ensuring *confidentiality*, the aim is to defend the "secrecy of information" (Lee, n.d.); that is, confidentiality ensures that access remains limited to only those who have been deemed privy. From personal communication with friends, and families, to private information shared with doctors, schools, businesses, and governments, securing the confidentiality of information also secures relationships themselves. In this way, ensuring confidentiality constitutes caring-*about* because it creates the conditions for caring-*for* to also be secured.

Likewise, ensuring the *integrity* of information "stops any unauthorized changes to data" (Lee, n.d.), which allows us to trust that data is accurate. This, too, serves as a form of caring-about because it creates the conditions for caring-for to be secured, as in the example of urgent medical data. Finally, ensuring *availability* "keeps services up and reachable for users" (Lee, n.d.). Whether these services are cell phone connections, email servers, or online banking systems, ensuring availability ultimately allows us to remain connected to one another. And while it is true that there is a wide spectrum of protections that fall under the CIA triad—some that more directly touch into caring-for than others—on a meaningful level, the CIA triad ultimately aims to protect trust in the information systems used to connect people with one another. In this, care theory's account of caring-about integrally connects with the work of cybersecurity in supporting the conditions for caring-for to be realized. Cyber space is, indeed, an extension of humanity and protecting cyber space also protects our connections to one another.

4. The Ethics of Care and the Technological Edge

Cybersecurity is uniquely positioned at the technological edge of emergent possibilities that are shaping society in dramatic and far-reaching ways. In opening into new possibilities, cybersecurity encounters unprecedented ethical challenges that far outpace established laws, regulations, and policies (Schneier, 2018).

This unique feature of cybersecurity exposes a limit to the efficacy of deontological—or duty based—ethical approaches that place moral value in actions that are justified in terms of pre-determined principles, laws, or maxims (Alexander & Moore, 2020). While the kind of "rational-objective thinking" that is at the core of deontological ethics has a place within care ethics, so too does "subjective thinking and reflection" (Noddings, 2013, p. 26). In proposing the ethics of care for the field of cybersecurity, we uphold this receptive mode of thinking as being particularly well-suited for responding to ethical challenges that emerge due to cybersecurity's position at the technological edge.

Noddings (2013) offers a compelling explanation on this point, saying, Starting the discussion of moral matters with principles, definitions, and demonstrations is rather like starting the solution of a mathematical problem formally. Sometimes we can and do proceed this way, but when the problematic situation is new, baffling, or especially complex, we *cannot* start this way. We have to operate in an intuitive or receptive mode that is somewhat mysterious, internal, and nonsequential. After the solutions has been found by intuitive methods, we may proceed with the construction of a formal demonstration or proof (Noddings, 2013, p. 7, emphasis added).

It stands to reason that Noddings' (2013) phenomenological description offered above comes close to what many cybersecurity researchers experience in encountering a new phenomenon—whether it be a new vulnerability in a system or a new piece of malware that is not yet understood. And, of course, along with encounters of novel technical challenges in cybersecurity, come ethical ties to people who depend on these technological systems in conducting their everyday lives. This feature of cybersecurity renders the "new, baffling, or especially complex" problems encountered in cybersecurity to be not only technical, but also inherently ethical.

Noddings (2013) notes a quality of engrossment that she says "must occur" in encounters of care (p. 17). Taken in conjunction with Nelsen's (2013) account of "the inquiry of care," a compelling description emerges that deepens the connections between the ethic of care and cybersecurity through a discussion of caring for objects and ideas in the process of conducting research. In particular, Nelsen (2013) notes, while caring for objects and ideas does not involve an ability to create a relation in the human sense, researchers can focus on how the objects of their research do indeed respond, albeit to notice and observe in this way requires an expansive notion of response. Likewise, the embodied nature of inquiry has implications for care-inspired research; it necessitates that all research be embodied (p. 366).

Accordingly, care-based inquiry unfolds through an intuitive process that incorporates both mind and body—feeling/thinking the way forward until the path becomes clear. This intuitive mode of proceeding also allows for connections with human and non-human objects of care to remain vital and alive, becoming an integral component of the process of inquiry itself (Noddings, 2013; Nelsen, 2013). Once this process of inquiry reaches culmination, a distinctly recognized logical sequence of steps can then be discerned in reflection (Dewey, 1997), completing the process and allowing for a formal, logically driven explanation to emerge. As such, the ethics of care engages with both rational-objective thinking and intuitive thinking and reflection. However, in the midst of confronting new and emergent problems, a mode of intuition-based thinking pushes inquiry forward.

5. *The Ethics of Care in Cybersecurity Practice: A First-Hand Example*

The ethics of care forwards a situation-based logical unfolding, rather than beginning with abstract rules and principles. From this contextualized starting point, the ethics of care proceeds through a perspective that takes personal responsibility for the basic well-being of others connected to the situation (Noddings, 2013; Engster, 2005). However, in the realm of engineering, the ethic of care also strongly connects with professional responsibility. Just as nurses take professional responsibility for the health of patients they treat, engineers take professional responsibility for the safety of the products they design (see further, Glennon, 1992). To illustrate this in the context of cybersecurity practice, we propose the following case study, put forth by the second author, based on his personal experience as a cybersecurity professional.

I was working for an organization that was subject to strict Food and Drug Administration (FDA) medical device regulation, with severe penalties for failing to meet the standards set forth by the regulating bodies. As part of my job duties, I was tasked with assessing a regulated legacy product that was widely used in health care settings throughout the United States to see what it would take to reproduce its functionality in the new cloud version of the product. While conducting my review of the product's codebase, I discovered that the regulated function was not meeting the minimum standards of non-repudiation for certain activities that had direct impact on the health and well-being of patients.

Curious and concerned, I began to dig a bit deeper. I then discovered I could delete log file entries, change attribution, modify date/time stamps and in general completely circumvent all security and audit controls. A catastrophic discovery at worst, and highly concerning, at best, I began documenting my findings in detail in order to present to the company's leadership. At this point, I was deeply concerned and acutely aware of the hundreds of thousands of patients who could be potentially harmed by the malicious use of the product.

Having every confidence that the leadership would take this discovery seriously and act accordingly, I worked the appropriate channels. Eventually, the issue escalated to the Chief Information Officer (CIO) and a meeting was scheduled to review the findings. As the day went on, I was excited to see how the team would addresses the issue. I was also looking forward to being involved in helping to come up with a solution, as this could be a great opportunity for growth in my career. The moment arrived and I walked into the CIO's office with all the top players present and all eyes on me.

I presented my findings and as I showed how I was able to circumvent all the security and audit controls, faces began to

drop—the pressure in the room changed. When I finished outlining the issue and demonstrating how to compromise the system, I was thanked by leadership for finding this and bringing it to their attention, as it was a very serious matter. I then shared that I had a potential fix for this issue and asked about who was going to be on point for this activity. I was told they needed some time to consider and would let me know.

I then asked when the company was going to get communications out to the necessary regulatory bodies about what had been discovered. Once again, the pressure in the room changed. I was told this was not a matter for me to be concerned with. I reminded them that there was a fixed amount of time allowed to report this finding to the respective regulating bodies or risk possible criminal charges. The response was astounding—the leadership team thought it was best to not say anything at all and I was told to keep this finding to myself. I reminded them that doing so constituted gross neglect and was criminal.

Because I had discovered it, I was concerned about the personal legal impact this could have for me and what this would mean for my family. I did not want to be charged with a crime. The leadership assured me that would not happen and that they would get the problem fixed at some point. Uncomfortable, but with no ability to do anything further, I left the room.

A few weeks later, I checked in on the status and was told that leadership had killed the project to fix the problem and said everything was fine. Concerned about the well-being of the company and the end-users of the product, I reminded them again that what they were doing was illegal. At this point, I was offered a promotion to a leadership role in a different part of the organization. I knew then and there they were trying to shut me up. I knew my only option moving forward was to submit my resignation. If I stayed, I would have felt responsible if anyone experienced harm because of this vulnerability. I couldn't continue to work under these circumstances. As I began looking for my next role, I was wrestling with what I was going to do next. I did not want to find myself in a similar position again.

I was frustrated. My purpose in doing this work was to protect people by protecting their information and the systems they rely on.Sadly, most of my colleagues were motivated by other things—they didn't even see the people. I knew in my heart I still wanted to work in infosec but was struggling to see how I was going to avoid winding up in a similar situation in my next role.That night my frustration hit its peak. I was disappointed with my previous employer and didn't respect the motivations of my industry. I recognized infosec was broken—it was set up to make as much money as possible, not to protect people.

That night I made a decision that would affect the rest of my life. It hit me like a freight train—why was I sitting back, waiting for someone else to fix things? I needed to step up to make the change. I dedicated myself to fixing the broken infosec industry and haven't looked back since. It isn't about information or security. It is about protecting people. My work from this point forward has been aligned with this mission. I get up every morning and work to make infosec work for people.

6. A Fundamental Ethical Paradox in Cybersecurity

Cybersecurity is an ethically vexed domain. In order to protect a system, cybersecurity professionals need to know where it is vulnerable. This means that cybersecurity professionals are on the lookout for ways to compromise a system. But once they find a vulnerability, the way forward can be complicated, to say the least.

There are many examples of this fundamental ethical paradox in cybersecurity, each one with distinct contextual details that shape the nuances of the situation. One notable example involves a tool called Mimikatz (Gentil Kiwi, 2014; Metcalf, 2015; Metcalf, 2018; Greenberg, 2017), developed by Benjamin Delpy, which eventually "became one of the world's most widespread and powerful password stealers" (Greenberg, 2017). When Delpy first discovered a vulnerability in "an obscure Windows function called WDigest" (Greenberg, 2017), he alerted Microsoft to the problem in 2011. At the time, Microsoft did not take the issue seriously, noting that in order for the vulnerability to be taken advantage of, a machine would need to be already deeply compromised. Delpy was not satisfied with this response and decided to code and release Mimikatz as a closed source program to demonstrate that the problem was indeed real. In Delpy's words, "Because you don't want to fix it, I'll show it to the world to make people aware of it" (as cited in Greenburg, 2017).

Taken at face value, it seems that Delpy's intention in coding and releasing the closed source version of Mimikatz was motivated by an aspiration to fix the problem, in an attempt to care-about the well-being of Windows users around the world. However, in Delpy's own words: "When you create something like this for good, you know it can be used by the bad side too" (as cited in Greenburg, 2017). In reflection he noted, "It turns out it takes years to make changes at Microsoft. The bad guys

didn't wait" (as cited in Greenburg, 2017).

The full story involves a stunning twist in which Delpy was pressured to hand over the full source code for Mimikatz to Russian spies at a security conference (Greenburg, 2017). "Delpy complied. Then, before he'd even left Russia, he published the code open source on Github, both fearing for his own physical safety if he kept the tool's code secret and figuring that if hackers were going to use his tool, defenders should understand it too" (Greenburg, 2017). Since this release, Mimikatz has been used widely by thieves and spies as well as cybersecurity defenders, underscoring how cybersecurity's interconnected, dynamic environment renders tools like Mimikatz double-edged swords. Given this, Delpy reasoned that releasing the open source code was the best way to balance the equation and give the good guys an opportunity to defend themselves against what was coming their way. Years later, it has been noted that "Mimikatz has done more to advance security than any other tool … " (Williams, as cited in Greenburg, 2017). And, over time, Delpy's release did lead to significant changes toward fixing the problem at Microsoft.

Analyzed through the lens of the ethic of care, this case shows how, taken at face value, the development and closed source release of Mimikatz was motivated by an attempt to care-about Windows users around the world in an attempt to pressure Microsoft to fix the underlying problem. However, once the full open source code was in the hands of Russian spies, Delpy deemed that the best way to offer care to the world was to fully release the open source code to the public. While the tool was subsequently used in powerful and widespread attacks, including NotPetya and BadRabbit, it has also led to significant improvements in cybersecurity (Greenberg, 2017).

Interestingly, at this macro scale concerning the well-being of everyone connected to the internet, care ethics comes very close to the reasoning that might be used in utilitarian ethics in considering the greatest good for the greatest number of people. However, at base, a key distinction holds in distinguishing the two paradigms at this macro scale; namely, care ethics' inherent motivation to care. Noddings expresses this distinction well in saying, care ethics' "emphasis is not on the consequences of our acts, although these are not, of course, irrelevant. But an ethic of caring locates morality primarily in the pre-act consciousness of the one-caring" (Noddings, 2013, p. 28). We, as humans, care because we care.

7. Education and an Ethos of Care in Cybersecurity

In a meaningful sense, cybersecurity is a realm in which good guys and bad guys are both playing with the same deck of cards—and, indeed, their moves are, at times, indistinguishable. Yet, there is a very real and critical distinction to be made from a moral perspective that distinguishes their actions. Thus, the relational context around actions—and not the specific actions in and of themselves—play a critical role in determining the moral valence of conduct in cybersecurity. On this point, pragmatist philosophy and feminist philosophy come together in an ethic of care that points to a broader ethos, or surrounding context, that shapes the meaning of actions taken in cybersecurity (Seigfried, 1991). This is a point that is especially critical in the formative introductions to cybersecurity that can transpire at critical points in children's development, as demonstrated in the case of Marcus Hutchins, "the hacker who saved the internet" (Greenberg, 2020).

Although Hutchins is now heralded as a hero for stopping what was, at the time, considered "the worst cyber attack in history: a piece of malware called WannaCry" (Greenberg, 2020), his initial introduction to hacking was shrouded in a veil of darkness and secrets. After being thrown into the spotlight for his work to stop WannaCry, Hutchins' past caught up with him and he was arrested by the FBI for his previous development of malware that was sold on the dark web years before he turned the corner toward white hat endeavors (Greenberg, 2020). In his youth, Hutchins was fascinated with computers, but was utterly bored in his school's computer class, where he was prevented from installing and playing computer games and was limited in the websites he could visit online. Being curious, creative, and cunning, the young Hutchins found ways around the school's attempts to limit what he could do on the school's computers, marking a critical point in his development where instead of cultivating and nurturing his budding curiosity and skills in a relational context—or ethos—of care, Hutchins was left, by default, to discover ways to cultivate his talents in a much different, darker, context (Greenberg, 2020).

The basic point that the relational context around action shapes the meaning of that action in significant ethical ways, upholds at all levels of cybersecurity education and practice. From the critical developmental years when young computer enthusiasts first discover hacking techniques, to the preparation of future cybersecurity professionals in higher education, as well as the ongoing culture that surrounds professional practice in cybersecurity, the relational context of these environments are foundational in setting the stage for action taken in cybersecurity. Here, the ethics of care contribute in ways that

are distinct from philosophical analyses of specific cases. By drawing out the kind of environment that should be intentionally cultivated at all of these levels in cybersecurity, the ethics of care describe a holding environment that can afford the field of cybersecurity a necessary degree of ethical cohesiveness that can endure as the field moves forward and confronts new ground (Blanken-Web et al., 2018).

8. Conclusion

On the surface, it may appear that the ethics of care stands at odds with the highly technical and often times, overtly masculine, realm of cybersecurity. Yet, in considering what it means to care, a strong argument takes shape that deeply links cybersecurity with care. In this vein, we submit the following definition of care:

On the most general level, we suggest that caring can be viewed as a *species activity that includes everything we do to maintain, continue, and repair our 'world' so that we can live in it as well as possible*. The world includes our bodies, ourselves, and our environment, all of which we seek to interweave in a complex, life-sustaining web (Tronto and Fisher, as cited in Tronto, 1993, p. 103, original emphasis).

In today's world, cyber domains constitute a life line that literally and figuratively maintains, continues, and repairs each aspect of the "world" mentioned above. In the realm of healthcare, digital platforms directly and indirectly make it possible for health care providers to care-for our bodies. Relationships are essential for maintaining ourselves,and in today's world, relationships are almost always at least sometimes mediated through the use of digital platforms, whether it be text, Facebook, Zoom, or email. And technology is ubiquitous in the environments we live in today. Indeed, most people would be challenged to go an entire day without interacting with something—whether it be a cell phone or even a refrigerator—that is connected to the internet. Digital devices have become a seamless part of the complex, interweaving, and life-sustaining web in today's world. And cybersecurity has a critical role to play in maintaining, continuing, and repairing this world so that we can live in it as well as possible. Cybersecurity is, indeed, inherently and deeply linked with care.

The ethics of care offer a different voice that can make considerations of cybersecurity ethics more robust. In putting forth this distinctly human approach to ethics, we aspire to shine a spotlight on a perspective that should be intentionally cultivated and included in considerations of cybersecurity ethics and cybersecurity practice alike. While we do not claim that the ethics of care should be the only ethical paradigm to consider in relation to cybersecurity ethics, we do believe that care ethics offer a unique contribution to the field and forwards a philosophical perspective that is worthy of being taken seriously for advancing ethical inquiry in cybersecurity.

References

[1] Alexander, L., Moore, M. (2020). Deontological ethics. *In*: E. N. Zalta (Ed.), *The Stanford encyclopedia of philosophy.* Metaphysics Research Lab. https://plato.stanford.edu/archives/win2020/entries/ethics-deontological/

[2] Azmak, O., Bayer, H., Caplin, A., Chun, M., Glimcher, P., Koonin, S., Patrinos, A. (2015). Using big data to understand the human condition: the Kavli HUMAN project. *Big data*, 3 (3) 173-188.

[3] Blanken-Webb, J., Palmer, I., Deshaies, S. E., Burbules, N. C., Campbell, R. H., Bashir, M. (2018). A Case Study-based Cybersecurity Ethics Curriculum. *In*: 2018 *{USENIX} Workshop on Advances in Security Education ({ASE} 18)*.

[4] Blanken-Webb, J., Palmer, I., Campbell, R. H., Burbules, N. C., Bashir, M. (2019). Cybersecurity Ethics. *In*: J. T. F. Burgess& E. Knox (Eds.), *Foundations of Information Ethics* (p. 91—101). American Library Association.

[5] Bradbury, D. (2017, August 16). *In search of an ethical code for cybersecurity.* Info security. https://www.infosecurity-magazine.com/magazine-features/search-ethical-code-cybersecurity/

[6] Christen, M., Gordijn, B., Loi, M. (Eds.) (2020). *The Ethics of Cybersecurity*. Springer Nature.

[7] Davis, B., Whitfield, C., Anwar, M. (2018, August). Ethical and Privacy Considerations in Cybersecurity. *In*: 2018 *16th Annual Conference on Privacy, Security and Trust (PST)* (p. 1-2). IEEE.

[8] Dewey, J. (1997). *How we think*. Courier Corporation.

[9] Dipert, R. R. (2010). The ethics of cyberwarfare. *Journal of Military Ethics*, 9 (4) 384-410.

[10] Engster, D. (2005). Rethinking care theory: The practice of caring and the obligation to care. *Hypatia*, 20 (3) 50-74.

[11] Friedman, M. (2015). Privacy, surveillance, and care ethics. *Care Ethics and Political Theory*, 108-126.

[12] Gentil Kiwi. (2014). *Overpass-the-hash* [article]. Blog de Gentil Kiwi. https://blog.gentilkiwi.com/

[13] Gilligan, C. (1993). *In a different voice: Psychological theory and women's development*. Harvard University Press.

[14] Gilligan, C., Snider, N. (2018). *Why does patriarchy persist?*. John Wiley & Sons.

[15] Glennon, T. (1992). Lawyers and caring: Building an ethic of care into professional responsibility. *Hastings Law Journal*, 43 (4) 1175-1186.

[16] Greenberg, A. (2017). He perfected a password-hacking tool—Then the Russians came calling. *WIRED*. https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/

[17] Greenberg, A. (2020). The confessions of Marcus Hutchins, the hacker who saved the internet. *WIRED*. *https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/*

[18] Hoppa, M. A. (2018). Automating Ethical Advice for Cybersecurity Decision-Making. In *Proceedings of the International Conference on Information and Knowledge Engineering (IKE)* (p. 170-171). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[19] Kenneally, E., Bailey, M. (2014). Cyber-security research ethics dialogue & strategy workshop. *ACM SIGCOMM Computer Communication Review*, 44 (2) 76-79.

[20] Knowels, A. (2016, October 12). *Tough challenges in cybersecurity ethics*. Security intelligence. https://securityintelligence.com/tough-challenges-cybersecurity-ethics/

[21] Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy*, 9 (3) 49-51.

[22] Lee, L. (n.d.). Cybersecurity Fundamentals. https://360.articulate.com/review/content/67330073-4c70-4c0e-9375-5d26670d99e7/review

[23] Leonhard, G. (2016). *Technology vs. humanity*. Fast Future Publishing.

[24] Lio, M., Christen, M. (2020). Ethical frameworks for cybersecurity. *In*: M. Christen, B. Gordijn, & M. Loi (Eds.) *The ethics of cybersecurity*. Springer Nature. (p. 73—93).

[25] Luck, M. (2019). Entrapment behind the firewall: the ethics of internal cyber-stings. *Australasian Journal of Information Systems*, 23.

[26] Manjikian, M. (2017). *Cybersecurity ethics: An introduction*. Routledge.

[27] Metcalf, S. (2015). Red vs. blue: Modern active directory attacks, detection, & protection. *Black hat USA 2015*. https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf

[28] Metcalf, S. (2018). Unofficial guide to Mimikatz & command reference. *Active directory security.* https://adsecurity.org/?page_id=1821

[29] Miller, S. (2019). Machine Learning, Ethics and Law. *Australasian Journal of Information Systems*, 23.

[30] Nair, I., Bulleit, W. M. (2020). Pragmatism and care in engineering ethics. *Science and Engineering Ethics*, 26 (1) 65-87.

[31] Nelsen, P. (2013). The inquiry of care. *Educational Theory*, 63 (4) 351-368.

[32] Noddings, N. (2002). *Starting at home: Caring and social policy*. University of California Press.

[33] Noddings, N. (2013). *Caring: A relational approach to ethics and moral education*. University of California Press.

[34] Pantazidou, M., Nair, I. (1999). Ethic of care: Guiding principles for engineering teaching & practice. *Journal of Engineering Education*, 88 (2) 205-212.

[35] Ramirez, R., Inagaki, S., Shimaoka, M., Magata, K. (2020). A Cybersecurity Research Ethics Decision Support UI. *USENIX Association,* (*August*).

[36] Samonas, S., Coss, D. (2014). The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security. *Journal of Information System Security*, 10 (3).

[37] Schneier, B. (2018). *Click here to kill everybody: Security and survival in a hyper-connected world*. WW Norton & Company.

[38] Seigfried, C. H. (1991). Where are all the pragmatist feminists?. *Hypatia*, 6 (2) 1-20.

[39] Shoemaker, D., Kohnke, A., Laidlaw, G. (2019). Ethics and cybersecurity are not mutually exclusive. *EDPACS*, 60 (1) 1-10.

[40] Tronto, J. C. (1993). *Moral boundaries: A political argument for an ethic of care*. Psychology Press.

[41] Webb, A. (2019). *The big nine: How the tech titans and their thinking machines could warp humanity*. Hachette UK.