

## THE FUTURE OF CYBER ETHICS

Marc Anderson

**Abstract:** This paper presents a survey of the conceptual development of cyber ethics, locating the main assumptions of the field up to now, and critiquing those assumptions. I argue that cyber ethicists have failed to understand that cyber arises from a ‘machine’ attitude to experience, which has given rise to computer-related technologies. Such technologies tend to be unethical by default, in terms of value. This drives the creation and idealization of cyber, as an antidote to the originating devaluation. Section 2 considers definitions of cyber ethics and their adequacy. Section 3 discusses the history of the term cyber. Section 4 outlines some historical and contemporary approaches to cyber ethics. Section 5 redefines cyber and cyber ethics and then goes on to offer some practical suggestions for the future of cyber ethics.

**Keywords:** cyber ethics, internet, digital technology, machine, value.

### 1. Introduction

The increasing influence of digital technology and more recently the connection of that technology to the internet, with all the problems they give rise to – social, environmental, and individual – have fueled a sustained and resurgent interest in developing ethics to help solve those problems. The development of that ethics has been approached from various angles, as (Sætra & Danaher, 2022) has shown, so that now there are a number of competing labels jostling for position in the same field, among them: cyber ethics, computer ethics, information ethics, digital ethics, internet ethics. In what follows I will reflect upon cyber ethics, recognizing that the other labels overlap, but in the hope that sustained reflection upon the *cyber* label in particular can give us new insights into the future of discipline.

I will not review the many categories of cyber ethics issues, nor will I discuss the current state-of-the-art thinking within them specifically. This has been well done already, by Spinello (2017) and others. I will note some of the main issues in cyber ethics indirectly and indicate how they stand with regard to the main thesis of this paper. The paper is about the future of cyber ethics, rather than the present. That future, as I will argue, depends upon recognizing the assumptions we make about computers and our understanding of ‘cyber-ness,’ and ought to be different than what has been advocated so far. I offer primarily a reflection on what cyber means, how it comes about, and how we can engage it in an ethically consistent manner in the future, based on a better understanding of it.

The thesis here is that *cyber as a concept and a practical result arises – mostly unreflectively – as an ostensible antidote to devaluations in experience brought about by a mistaken tendency to approach that experience in a ‘machine’ manner. The primary example of this ‘machine’ approach is the devel-*

*opment of computer technologies. To be successful, cyber ethics will have to recognize the devaluation inherent in computer-related technologies and work to correct it, i.e. to attenuate and offer alternatives to 'machine' thinking.*

I begin, in Section 2, with definitions of cyber ethics, followed by a reflection on their adequacy. From there, I go on in Section 3 to discuss the history and sources of the term cyber itself and then draw out the assumptions disclosed in that history. In Section 4 an outline of the original historic attempts at cyber ethics is given, followed by a survey of some contemporary accounts. Section 5 then attempts a redefinition of both cyber and cyber ethics, based on insights developed in the earlier sections, and goes on to offer some practical suggestions for the future of cyber ethics. A conclusion sums up the effort.

## **2. What does Cyber Ethics Mean?**

### **2.1 Some Contemporary Definitions**

There is no well-agreed-upon definition of Cyber Ethics, although various attempts have been made. Tavani for example, states that: “cybertechnology . . . [is] the entire range of computing and communication systems, from stand-alone computers to privately owned networks and to the internet itself. ‘Cyberethics’ refers to the study of moral, legal, and social issues involving those technologies” and further, “Cyberethics examines the impact of cyber technology on our social, legal, and moral systems, and it evaluates the social policies and laws that have been framed in response to issues generated by its development and use” (Tavani, 2015, 2). This definition thus centers around a technology – computers and communication systems – as something *external to human action, but according to which human action changes or is molded*. This definition is somewhat passive or descriptive tending, as being primarily *a study of effects rather than a development of recommendations to change behaviors*.

Sakka and Spyrou, note one definition of cyber ethics as: “the code that gives guidelines for the proper behaviour on the Internet” (2015, 647). Here the definition is undertaken in terms of *a region, which one can occupy*, much as one might say that marine ethics would deal with behaviour ‘on the sea.’ Moreover, ethics is explicitly linked to a *rule structure* within this region and a *codification* of that structure, and thus to historical tendencies toward codification, professionalism, and legal outlook (the crystallization of moral norms into socio-legal duties).

Finally, a third definition makes out cyberethics to be: “the moral choices individuals make when using Internet-capable technologies and digital media” (Pusey & Sadara, 2011, 82). The emphasis has here shifted to *an internal perspective*, neither the study of effects nor externalization of actions, but now *on the initiation of actions either in relation to the relevant technologies or within the regions* created by such technologies.

### **1.2 Are the definitions Adequate?**

The definitions thus disagree on what aspect of the technology is in view: *its effects, the context it creates, or the dilemmas and possibilities it offers* to its users. But they also disagree on the level of practice involved in engaging the technology ethically: *descriptive study, explicit framing, or individual choice*. They are thus practically inadequate, at least in terms of consistency and complexity. We might argue that all of these various assumptions and approaches are worthwhile, the approach of ‘a little of everything.’ On the other hand, if we find ‘a little of everything’ unsatisfying in terms of clarity, we might attempt to find a connecting thread through these various insights.

A promising place to begin might be to consider what *cyber* adds to the term cyber ethics. Directly engaging the meaning of the term cyber itself might then lead us to disclose whether there is something hidden in the notion of cyber ethics, which is not disclosed as well in nearby terms such as information ethics or digital ethics.

## **3. Sources of Cyber:**

### **3.1 History and Etymology of the Word**

The use of the term *cyber* predates Norbert Wiener’s use of it in *cybernetics*, as he noted. It derives from the Ancient Greek *κυβερνάω*: to steer literally, or metaphorically, to guide or govern (Liddell and Scott, 1883, p. 854). Wiener used the term in order to describe the ‘complex of ideas’ gathered around

the theory of messages including “not only the study of language but the study of messages as a means of controlling machinery and society, the development of computing machines and other such automata, certain reflections upon psychology and the nervous system, and a tentative new theory of scientific method” (Wiener, 1950, 15).

Some of the foundations of how we now use the term *cyber* is thus present in Wiener’s use of the full term, but the latter is also visibly more and less than the way we use it. In the first place, the Ancient Greek notion of governing or steering has now been watered down or even lost. In the second place, a notion of disembodiment and otherworldliness has pushed its way into what we mean by the term.

Cambridge Online dictionary defines the adjective *cyber* as: “involving, using, or relating to computers, especially the internet.”<sup>1</sup> But this description misses the sense of disembodiment which accompanies many uses of the term. To add *cyber* to a word now evokes not its use in relation to computers, or to the internet simply, but a sort of placement in a digital region or realm beyond physicality, or rather beyond the type of confines which often accompany physicality. An example: the word computer generally often stands for an item of digital hardware such as a laptop computer. If you then go on to add cyber, i.e. *cybercomputer*, you push the physical computer into this digital, unreal, physically invisible, or *virtual* realm,<sup>2</sup> e.g. in its use by (Hahanov et al., 2011).

Thus, the current notion of cyber is not covered by its *mere* computer-relatedness at least. If it is not covered by computer-relatedness, then it is arguably also not covered by internet-relatedness. The latter can equally refer to the technological framework or system, historic and current – and in some ways very little changed from its inception – which is an extension of computers and thus of computer relatedness. If that system remains static, then cyber will be something still further beyond it; it need not be a spatial beyond, but it is easily characterized in spatial terms by habit, as we shall see. But if the internet is not static,<sup>3</sup> then nonetheless the pushing beyond remains the core of the relation. In short, cyber is not digital technology nor an extension of that technology, it is a way of thinking, brought about by that technology. It is this way of thinking and what it entails, foremost, that calls for ethical reflection in terms of futurity.

But how did we get to the current use of the term cyber from a mode of use by Wiener? As with many human words, the route appears to be a gradual warping of some original use due to seemingly arbitrary circumstances. In this case, half of Wiener’s term was taken up by a corporation, Control Data Corporation (CDC), as a name for its range of mainframe computers, the CYBER line of computers began in 1971. CDC was also using the registered term CYBERNET (Cyber 70 Computer Systems Product Announcements, 1971).

By the late 1970s other businesses and US government agencies such as Defense Technical Information Center and NASA, were using the term more loosely based on their use of CDC Cyber mainframes. Later in 1981, Byte magazine used the term Cyber in mainly lowercase to stand for the CDC CYBER 170 in articles describing programming techniques related to the CYBER line of computers (Sedlet & Dust, 1981, 472). By 1984 Antic Magazine (New Products, 1984, 102) was advertising a graphics utility product called CYBER Graphics under new products.

At that point the term had clearly become a way to add mystique to products related to the computer hobbyist world, but products which were increasingly also aimed at a more general buying public. Through the mid-1980s the term’s use was multiplying as a term naming products, including games. By 1990 the term had found its way into science fiction as well as investing, and turned into small c cyber, and already – in the word cyberspace, which William Gibson had used in *Neuromancer* in 1984 – had begun to take on the popularized sense of a virtual place ‘beyond.’ In using it in a review of an encyclopedia of post-modern thinking, Fogel (1989) for example, spoke of “hyper-images clogging cyber-space”, i.e.

<sup>1</sup> <https://dictionary.cambridge.org/dictionary/english/cyber>

<sup>2</sup> The word *virtual*, now also used in a sense similar to that of *cyber* with regard to digital technology, was often used by medieval philosophers – *virtualis* – to describe essence or efficacy without actuality, showing that the weight of interest in the concept sought after is thus strong enough to issue in various ways.

<sup>3</sup> One can distinguish ‘internet’ from ‘World Wide Web,’ and now – which increasingly replaces it: ‘online’, though these terms are increasingly blurred in public consciousness and use.

to the use of the computer to move to images beyond the user interface region, in a beyond which nonetheless has relations and limits – because it can be clogged – derived from its origins. Finally, by the late 1990s, the term transitioned more fully into the sense in which we now have it. Meanwhile, alongside this, Wiener's term cybernetics continued to be used in narrower contexts, but without becoming widely popularized.

### 3.2 Assumptions

We have seen that the originating notion behind cyber in Wiener's cybernetics, governing, and the later use of cyber as an adjective – moving into the virtual beyond – diverged. Yet they did not diverge arbitrarily perhaps. Governing was central to the earlier conceptions of automated systems. Control systems governed and were governed by the messages which had begun to be passed through electrical wires. The human was viewed from early on as a prominent part of these control systems, and yet viewed ambiguously both as a dispensable part, indeed a component part, and as a controlling element, e.g. (Anderson & Fort, 2022).

This ambiguous sense of the human role in control systems is not lost in contemporary views about the relation of humans to digital technology and the internet. It arises from the assumptions which give rise to technologies and Wiener was one of those who clearly articulated those assumptions. "When I give an order to a machine, the situation is not essentially different from that which arises when I give an order to a person ... the fact that the signal in its intermediate stages has gone through a machine rather than through a person is irrelevant" (Wiener, 1950, 16).<sup>4</sup>

On this assumption the status of the human relative to the system becomes ambiguous. If, for the purpose of messages, person or machine status is irrelevant, then systems that incorporate humans and machines are indistinguishable practically from those that merely incorporate machines. Moreover, giving an order to the machine – i.e. 'ordering' or governing the system – is itself a signal, thus subject to the same considerations of irrelevance, and thus setting up a human-machine system in its own right that includes the one giving the order. In this view, each use of a machine is infected with this irrelevance. I do not give orders to a machine, any more than by – ostensibly – giving orders to it I simply become part of a human-machine system.

With this ambiguity it becomes difficult to separate a *control of experience*: a narrowing of options for interpretation directed at some region of experience, from a *guiding of experience*: an expansive offer to interpret experience directed at some region of experience. The former is an imperative attitude of e.g. 'Do this!' The latter is a teaching attitude of e.g. 'consider one of these'. The former approach means to duplicate one's own already developed or embedded meanings onto the 'outer' experience, e.g. the consciousness experience of some other human, whereas the latter invites the meanings of the other to intermingle with one's own meanings in some new and creative way.

We can go a step further though. On the above terms *machine* – and computer technologies above all<sup>5</sup> – can be defined as a sustained manipulation of experience that is amenable to controlling engagements to a far higher degree than other modes of engagement encountered in the average of experience, including guidance. In other words, 'machine-ness' in any area of experience is just the degree to which that experience has been primed to accept interpretations that have been already established. Or again, 'machine-ness' is an aspect of things in which some locus that makes interpretations – e.g. now usually a human but perhaps in the future an autonomous device – can copy 'its own' experience, forcing it on another region of experience. Not *en bloc* usually, but selectively. It is a way of ensuring that you get the *same* results over again in some area of experience to the degree that you want the sameness of results. Mechanical factory machine-ness 'stamps out' the same industrial parts over and over. In themselves, by default, computing machines do something similar in their medium.

This takes on a social sense insofar as human action can also be squeezed into forms of machine-like behavior. If ethics is defined axiologically, in generalized terms, relative to the *value in experience*, then machine-ness immediately becomes a tendency that 1) molds experience into quantitative – repetitive –

<sup>4</sup> Wiener's title – *The Human use of Human Beings* – is quite appropriate:

<sup>5</sup> Computers, in their precise logical stepwise processes, are our highest expression of a mechanical control of experience.



types of value, and 2) cuts off access to more creative – less repetitive – varieties of value. Thus, contrary to Wiener's assertion that "in control and communication we are always fighting nature's tendency to degrade the organized and to destroy the meaningful," (Wiener, 1950, 17), it is arguable that in degrading organization, nature in fact works *against* devolutions into certain simplistic varieties of value bound up with the machine-ness tendency.

But that is a story for another day. The point here is that the notion of a disembodied virtual realm, a 'beyond-ness' or digitally informed way of being, a *cyber-ness* – the actual word used is a somewhat arbitrary development as we saw – arises naturally from this notion of machine-ness. If you set up a 'machine world' of computer technology, along the lines of machine-ness as described above, either actually or in imagination, then you immediately also set up the notion of the antidote relative to that world: a region in which interpretations of experience break out to remain relatively free and merely guided, rather than squeezed, controlled and run stepwise and 'clockwise,' i.e. according to clock timing.

There is thus a push and pull involved in engaging computer technology. In using it we are drawn – pulled – in as another component which, in controlling and being controlled, facilitates the system and becomes nothing more than a part of it. But this state pushes us to idealize beyond the technology and seek – but still in relation to it and in ways that incorporate certain aspects of it – for a realm that merely guides interpretations of experience relatively freely. The latter is *cyber-ness*, which we can define tentatively and informally as: *the actual and idealized realm/context of comparatively free interpretation of experience arising in response to the devaluations brought about by the adoption of machine-ness assumptions and their development into digital electronic computer technologies in particular.*

Cyber-ness is by no means limited to being a response to digital computer technologies, except insofar as cyber is the word currently used to evoke it. Works of H.G. Wells, such as *The Time Machine* and *The War in the Air*, clearly display the urge toward cyber-ness. They are cousins of the more contemporary push away from the assumptions of digital technologies but arose from similar tendencies embedded within the 19th-century industrial revolution (variant of) machine-ness: a world of iron, steel, cogs, and levers. More proximally in time, the hobbyist feeling surrounding home computer use and building in the 1970s and 1980s, and the 'promise' of what could be done with such machines, e.g. (Campbell-Kelly et al., 2018), was another form of this cyber-ness. The roots of this push and pull are in the structure of the experienced world as a realm of interpretable experience, amenable to value-aware ethical engagement.

Cyber or cyber-ness in the sense above could thus be characterized as a relatively ethically 'good' outcome of computer technology, while machine-ness could be characterized as a relatively ethically 'bad' aspect that gives rise to that technology. Insofar as we are able to break out into interpretive freedom relative to it, everything that computer technology allows us to do then, or which we project it to lead to in a promising computer technological future, falls under the aegis of cyber.

To repetitively buy, charge, worry about, and stare intently for extended periods into the small glass screen of a cell phone developed by machine assumptions, is the technology's narrowing of interpretation in machine-ness. To then break out into a virtual realm where music, videos, events, and multiple friends, confederates, and allies, over relatively long distances, and at flexible times, are ready to be interpreted, is the cyber 'release' from the aforementioned narrowing built into the cell phone and its use. The unethical narrowing tendency is, of course, amenable to local expansions, e.g., the work conditions of cell phone factory workers *could* be improved, while the expansive tendency is, without care, liable to localized narrowings of experiential engagement, where machine behaviors such as replication are exported into the cyber realm, e.g. re-tweeting tweets.

## 4. The Development of Cyber Ethics

### 4.1 Historical Approaches

We can follow the trail of this push and pull through the 70-year history of computer technology development in terms of the ways in which ethicists have attempted to grapple with it, without perhaps quite understanding its roots.<sup>6</sup>

<sup>6</sup> In fact, the trail could be followed much further back into the history of the attempt at 'machine thinking' in calculus and logic, and into the forms of medieval scholasticism and beyond, but that would take us too far

Wiener's reflections make a good starting point, as I have suggested earlier, for the tensions inherent in the assumptions about control system technology are already found there.

For Wiener already 'we as a society are our messages.' (Wiener, 1950, 18). Messages are a form of decreasing entropy - local areas of organization - so that "in both the animal [and the human] and the machine this performance is made to be effective on the outer world. In both, their *performed* action on the outer world, and not merely their *intended* action, is reported back to the central regulatory apparatus" (Wiener, 1950, 27). On the other hand, in his discussion of human social structure in comparison to that of ants we read, unsurprisingly, that: "if the human being is restricted to perform the same functions over and over again, he will not even be a good ant, not to mention a good human being" (Wiener, 1950, 52).

Here's the rub though: the price of the former is the latter. In other words, the mechanisms by which more complex versions of such communication loops are achieved are the actualizations of a devaluing 'restriction to performing the same functions over and over again.' You cannot expect to get a message back unless you set up conditions to get messages back. You do not develop systems arbitrarily on one side in the mere hope of getting messages back. You get such messages back because the system on the sender side, and that of the received/resender side, has developed in tandem, not merely physically but conceptually. A great many of the issues central to cyber ethics can be shown to develop out of this constrictive implication of control, with the tension carried on into the gradual and explicit development of computer ethics accordingly.

In 1985, about the time that the term Cyber was expanding beyond its use as a label for CDC main-frame computers, James Moor wrote an article in which he defined computer ethics as: "the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology" (Moor, 1985, 266). Here policy is pre-eminent and ethics is envisioned as feeding into it.

But notice that it is the very existence of computer technologies that creates what Moor calls a *policy vacuum* in which we are faced with *new choices for action* (Moor, 1985, 266). In other words, the view of the main problem for ethics follows the thread suggested above: the nature of the technology opens up a realm beyond – both actually and potentially – which is then liable to be engaged in unethical ways – insofar as they extend the assumption of machine-ness into this 'free' realm and destroy it. As Moor puts it: "Because computer technology provides us with new possibilities for acting, new values emerge" (Moor, 1985, 267). This is true in a specific sense of values, but it is also therefore true in a generalized sense of *value* mentioned above, as well.

For Moor, computers are revolutionary, and computer ethics has a special status. But this is not because of their ubiquity, their newness, their ease of use, or their ability to manipulate numbers. It is, he states, a result of their logical malleability in terms of "the number and variety of possible states and operations ... [and the fact that] the states of the computer can be taken to represent anything" (Moor, 1985, 270). By 1985 computers had only spread and been popularized a fraction of how far they have now, thus this 'free beyond' in which they would eventually spread and all of the possible applications they could be used for, was a shimmering cyber vision on the horizon.

In later contemplating this cyber horizon – though he doesn't call it this – as a realm that will be filled, thus pushing beyond the question of 'what can we apply computer technology to?' and spilling over into 'why do we do what we do here?', Moor provides an insight into how the limitations of machine assumptions act. Similarly, to its namesake in the Industrial Revolution – which Moor unsurprisingly evokes – machine thinking spreads, causing us to continually push beyond it in cyber-ness.

By 1997, the cyber beyond had begun to take a more definite shape, so that Deborah Johnson could discuss ethics in terms of being online. According to Johnson, several special features of online communication give rise to ethical issues. There is the speed, immediacy, and reach of communication (scope), the anonymity of such communication, and its reproducibility (Johnson, 1997).

The ethical problems identified under each of these aspects can all be understood in terms of the machine-ness versus cyber distinction. The varieties of scope noted by Johnson, for example, are

---

afield. The tension in question is not limited to technology as we usually understand it.

variants of the urge to bring machine assumptions into the evoked cyber realm, which can be seen in Johnson's characterization of scope as power. In terms of communication, scope as power, is the ability to force interpretations upon others, i.e. force others to participate in some experience in quantitative and repetitive value.<sup>7</sup> Online and email spamming exemplify this perfectly.

Johnson also notes that we restrict other technology uses but not online actions. She forgets, however, that most other technologies were not in fact regulated until their problems became apparent, which in some cases took 20 or 30 years after their first commercial successes. The chaos of the early use of automobiles, described by Loomis (2015), provides a good example here. The online realm, similarly, was not restricted in Johnson's time because it was still newly cyber. It is becoming increasingly restricted, however, not merely by legal regulation, but by the narrowing off of interpretation in the preponderance of commercial actions, pre-eminently those of big tech.

Anonymity and reproducibility are likewise issues of loss of control, over material put online. To be able to reproduce/replicate, e.g. a message, is one of the things computers are *developed* to do easily. Reproducibility is a variant outcome of machine assumptions. When someone merely reproduces a message originally created online by another – the byways of big tech social media have increasingly promoted this – they participate in this machinelike behaviour, which is ethically destructive as a tendency in relation to the cyber realm. The ultimate outcome of such actions is intuited – and was intuited relatively early on as we saw above in Fogel – as a 'filling up' of the online realm: a destruction of its cyber-ness. The extent of the latter is increasingly evident in the contemporary filling up of online space by social media giants, with mass advertising, etc.<sup>8</sup>

Ironically, the message can also be commandeered and creatively re-interpreted, which is a valuating tendency. This arises in response to the pushing of machine-ness into the cyber realm and accounts for the mystique of the hacker. Indeed, Johnson nicely highlights this process, alluding to the Wild West view of cyberspace which was used as a metaphor at the time. The historic Wild West was, at least in idealized form, free and lawless. Accordingly, she laments that: "our primary response to behavioral problems online has so far been legal and technological," and suggests ultimately that "we can have a variety of forms of online communication with a high level of trust if the rules are known or explained to individuals before they enter an environment" (Johnson, 1997, 60; 65). But since machine assumptions are a form of control, this is an obvious evolution: either machine-like assumptions of social control are introduced into the cyber realm through efforts at controlling behaviour (legal efforts, codes of conduct, etc.), or the near elements of the computer machine processes themselves, such as software, are pushed into the cyber realm (technological efforts). In either case, the cyber realm is diminished as a 'space' for free interpretation, and this struggle between the encroachment of machine assumptions and the realm of cyber envisioned as free generates ethical issues.

As computer ethics, and now cyber ethics have progressed, the location of the tension between machine assumptions and their cyber antidote has shifted. Terrell Bynum, for example, in 2000, raises one of the more metaphysical ethical questions regarding computers, and one which has particular resonance with modern popular thinking on AI development, namely, if we develop machines like us or surpass us in intelligence, will they have rights? (Bynum, 2000, 10).

Assuming, according to Bynum's conditions, that the comparison remains a comparison with humans,<sup>9</sup> then we can see that to ask the questions *at all* is to have an unconscious intuition of the source of the ethical problem as described earlier. In other words – all things being equal – we would not arbitrarily pick a human from among other humans and ask: "Does this human have rights?"

<sup>7</sup> Both Moor and Johnson mention value – and the latter even mentions disvalue – which is a step in the right direction for gaining a clear prospective of cyber ethics, although they do not engage with the notion in a sustained manner in the articles in question.

<sup>8</sup> The online space is not an 'infinite' space to be filled, so that one might say it is a moot point since there is an endless beyond to it to be engaged. Rather, as it fills, the filled part clogs up the access to the still unfilled beyond.

<sup>9</sup> And not, for example, one with animals, where the capacities of the latter are seemingly unlike ours.

The source of the problem lies in the difference in the arising of the machine in comparison to the arising of a human. Its arising depends upon higher degrees – relative to a human – of *replication, construction as variations of replication and control of externality*,<sup>10</sup> and *inability to respond with relatively free interpretations*. Bynum gives away the key to the problem, indirectly and inadvertently, in the following phrase “[some] might argue that human purposes and human justice must prevail over those of ‘mere machines.’” (Bynum, 2000, 10) What are *mere machines*? *Mere machines* will be intuited as such only because of their relative similarity, the way their processes are known to develop, or the degree to which they must follow impositions of external control. Insofar as these limits do not apply, we will not distinguish them from, e.g. humans. Insofar as they will not incorporate *machine-ness*. They are machines, and mere machines, because we are aware of the machine assumptions in the actions which have developed them.

By 2000, cyberspace also came to be understood as a realm in which dominations of space from the external world are recreated (Quina & Miller, 2000). The latter authors are much more aware of the imposition of the forms of control extant in ‘external’ reality – one of which is the historic varieties of male dominance – on the ostensibly free realm of cyberspace. And this insight is not particular to the specific ethical issue engaged by Quina and Miller. (Nooney, 2021) skillfully details how, through a “decades-long drama between body and machine,” computer technology has broken our bodies – a burden born particularly by women in the late 20th-century office workforce – by narrowing our physical/spatial freedoms to fit the demands of the technology. This narrowing of physicality by the machine only exists, however, by allowing the lure of something on the cyber ‘other side.’

The debate between those who envision a free online realm, as illustrated for example in the French *libriste* software culture, and those who would export the machine control assumptions of the physical world into the online realm, gets its beginning in the intuitive but often unconscious recognition of machine versus cyber thinking. (Guerry, 2001)<sup>11</sup> notes the close relation between the hacker concept and the free and open-source software movement. This is no accident.

(Goodwin & Rogers, 1997), in discussing cyberpunk as a sci-fi concept rooted in the economic situation of the 1980s, characterized cyber negatively, as the technological devices invading physical embodiment and the technological systems controlling humans. They were right in noting that cyberpunk is a science fiction genre that depends upon the ‘projection of the present.’ On the other hand, I suggest that they misunderstood just what was being projected and thus were mistaken in characterizing cyber negatively.

The cyberpunk world, as they outline it, pits the order of technology against the chaos of those opposed to it. The order is externally imposed through the control of information. Moreover, virtual reality, a major element of cyber, serves as a means of escape from that control and confinement, and ‘cyberspace cowboys’ manipulate that free realm and create uncertainty. If this sounds familiar it is because it is the very concept of machine-ness at a more general level that is evoked.

But the free realm beyond – of cyber – confers the air of ‘hero’ upon those who can thrive in it, i.e., can bypass the control assumption in all its machine forms – one form of which is indeed *the setting up of the laws of the physical world in the realm where the technology resides*. The heroes are thus ‘criminals,’ with regard to control, and yet relatively ‘good’ in the very specific ethical sense under discussion. As Goodwin and Rogers put it, the ‘heroes’ of the world of cyberpunk: “do not accept the confining circumstances of their world” (Goodwin & Rogers 1997, 45). This is precisely the promise of the cyber realm and well describes the ethical thread that runs from the machine-narrowed realm of the computer technology-saturated real world to the cyber realm.

<sup>10</sup> To the extent that cloning humans becomes practiced, if ever, then the very same ethical problems will apply to human clones and for several of the same reasons suggested: they would be constructed from ‘without’ and they would be known to be replicates.

<sup>11</sup> And more recently with the ‘Blue Hats’ open-source hacker community to which Guerry belongs. <https://www.numerique.gouv.fr/actualites/la-communaute-blue-hats-hackers-dinteret-general-est-lancee-rejoignez-nous/>



#### 4.2 Contemporary Approaches

What then of newer cyber ethics approaches, do they also indicate a tension centered around the notions of machine control and freedom from that control? A survey of them indicates that they do. Alhassan et al., for example, state that Cyber Ethics: “is about societal accountability in cyberspace. This comprises a set of standards which recommend morality in cyberspace, considering the preservation of freedom of expression, intellectual property, and privacy” (Alhassan et al 2020, 2). On this characterization, cyber ethics is not grounded in *what* you do in cyberspace or *how* you do it, so much as it is grounded in *the very act itself of carrying into cyberspace the (social) assumptions from the physio-technological realm*, including those which govern work and technological design.

In other words, the view is that the cyber realm cannot be left free of those assumptions if it is to be ethical – it cannot be a ‘realm beyond’ in which there is full freedom to do as one will. But this view immediately gives rise to contradictions, most obviously, that freedom itself is to be preserved in the cyber realm, but also, and more importantly, that there is no inherent limit to carrying these assumptions into cyberspace. The latter means that cyberspace is continually eaten away, causing us to go further in envisioning a ‘cyber plus’ beyond cyberspace. It also brings us up against the hard reality of our physical world and its sustainable and environmental limits, for an expanded cyber beyond rests upon an increasing but unsustainable and environmentally devaluative physio-technological expansion in the physical world.

One might respond that these contradictions are inherent in all experiences within the physical world, regardless of technology. This is correct. It suggests however that our efforts at ethical engagement in cyber will fail unless we understand what the cyber realm is and how it arises and unless we modify our ethics. That modification will not be based upon merely exporting variations of the control assumptions that find their most complex technical expression in computer technologies into the cyber realm.

Those very assumptions have created the urge for and the fact of the cyber realm. Exporting them into that realm will merely create a further need and spark a new effort to be released from them in their new guise, by advancing to something ‘beyond cyber.’ The trend of contemporary cyber ethics is attempting to do just such an exportation however, in such approaches as: codes of ethics, anchorings of cyber ethical issues in the ‘real’ physical world, frameworks, and legal-ethical hybrids.

Codes of ethics have been attempted since the medical Hippocratic Oath. They have proliferated well before computers, in disciplines that were tied more closely to the physio-technological realm as an area to apply technological control assumptions. In engineering, for example, one can find proto-codes of ethics going back 140 years or more, e.g. (American Institute of Electrical Engineers, 1907). These codes engage the physical instantiation of control assumptions: responsibility, standards, safety, etc. Cyber ethics code efforts, such as that of the ACM and IEEE (Gotterbarn et al., 1999) proceed from the very same base: control assumptions are to be imposed upon the designer or user physically designing and manipulating the computer technology. In other words, the first attempt is to regulate (control) the ‘gate’ to cyber.

Another approach, such as that described by (Haigh & Jones, 2007), relative to the ethics of research in the cyber realm, is essentially one of anchoring ethical engagement in cyber in the ‘real’ physical world. This involves, in general, pulling activity in the cyber realm back ‘out’ of cyber, to be reviewed or confirmed by ethics committees. More specifically it involves such moves as backing up cyber/virtual consent with physical proof, and un-disguising default cyber realm anonymity.

Tellingly, Haigh and Jones feel compelled to admit several times that these moves are inconsistent with the nature of the cyber realm, noting e.g. that “the consent process must not be perceived as disruptive to discourse in the virtual world” (Haigh & Jones, 2007, 80) and “[real world consent] can be seen to undermine the borderless nature of the world-wide-web” (Haigh & Jones, 2007, 81) This readily highlights the tension between machine control assumptions and the intuition of what cyber is as a supposed escape from those assumptions. The characterization of the cyber realm by these authors as having levels of depth, with ethical dilemmas being superficial at upper levels – public web spaces – and highly significant at lower levels – virtual realities – highlights that tension even further (Haigh & Jones, 2007, 83).

I suggest that the foregoing characterization is only possible because the ‘upper’ levels are viewed as remaining connected, through real-world data, which is subject to real-world control assumptions, to the physio-technological gateways that give access to cyber. Thus at ‘upper levels’ the control assumptions proper to the technology and to a control-oriented and negative ethics – more on this later – remain in place and active, thus dispensing, relatively, with the need for new ethical engagement.

Zhang et al. (2022) serve as another particularly interesting example of the tension in question while discussing cyber ethics in terms of platial (place-based) research. This is because embracing an emphasis on place as opposed to location (with its boundedness and amenability to control assumptions) *should* pave the way to recognizing that cyber ethical concerns that arise precisely because of the cyber possibility of non-locatedness are not likely to be fruitfully engaged by ethical approaches grounded in that very locatedness. Unfortunately, the authors give no indication of such an insight.

The idea of platial research at all *is* an ethical response in the right direction, and one that should be recognized as such relative to the cyber realm. Rebuilding interpretive links to types of experience beyond the mere quantitative and controlling engagements of locatedness – which computers manipulate oh so easily – is rebuilding value, as qualitative. So far, they are on the right track.

However, the authors go on to note how surveys show that maps that display private locations are regarded as unethical, with the main worry being that the identification of individuals facilitates risks from criminal or hacking activity. To note this is to highlight how the exportation *as such* of physical-empirical elements into cyber is viewed as unethical, along with unethical tendencies bred in the former, e.g. the possibility of being attacked, harassed, etc. once one’s location and movements are freely known.

In other words, the fear again, ethically, is that the control assumptions that prevent or limit such criminality in the outer ‘real’ world – e.g. law, regulations, etc. – are absent in cyber. This assumption is just what we have seen in other authors and it leads to solutions such as: providing advanced geomasking techniques, instituting and strengthening frameworks and committees, adopting principles specific to the field, and above all the exportation of external citizen behaviour into cyber, with the presumption that vaguely participatory moral-democratic behaviour can be transferred into the latter (Zhang et al., 2022, 90) But once again, this is inconsistent with the very notion of cyber, which arises and gets its sense as an *escape from control assumptions*.

Reviewing cyber ethics from a behavioural perspective, (Aderibigbe, 2021) highlights a number of approaches that engage it in the manner under discussion. Intellectual property ownership is cited as a major issue for example. The commodification of intellectual property is arguably a result of machine thinking, however: intellectual property as an object. And yet the commodification of intellectual property through machine control assumptions, i.e. intellectual property making the move toward being a mass manufactured commodity, must be reconciled with the fact, as Aderibigbe states, that: “human behaviour is classified into two separate but interrelated worlds: real-world behaviour and cyber behaviour” (Aderibigbe 2021, 274).

Real-world behaviour under machine assumptions is what is creating the problem for intellectual property, however. Thus, the various types of efforts, Aderibigbe mentions, e.g. control of behaviour, tools derived from the Theory of Planned Behaviour in order to control behaviour, perceived behaviour control, emphasis on control by law, and acceptable use policies (a form of real-world contract signing which unsurprisingly has no teeth *in* cyber), are simply bandages which do not get at the heart of the problem.

As we have seen, in cyber ethics considerable emphasis is placed upon law and variations of law in the world of physical experience. Again, this is predictable. Spinello, commenting upon Lessig’s notion of constraints that limit our behaviour in ‘real space’ – laws, norms, market conditions, and architecture, accepts that “in cyberspace, we are subject to the same four constraints” (Spinello, 2017, 3). Spinello is right in suggesting, further on, that ethics is distinct from norms. Yet I believe he misses something important, namely that cyberspace – and cyber – arise because of a particular variation of the noted constraints, a variation which achieves a relatively complex perfection in our act of creating computer-machine technology.

Thus, ethics cannot remain *meta*, as Spinello characterizes it, if it is to achieve results. In order to advance it must be turned upon the whole set of machine control assumptions which give rise to cyber and cyberspace. It must be used to rethink machine control assumptions as such. Without such a turn we will remain stuck in *an endless cycle of contradiction, in which we fruitlessly attempt to solve ethical problems which are embedded into the very assumptions behind the development of computer technology*.

## 5. Future Cyber Ethics

### 5.1 Redefining Cyber and Cyber Ethics

A new definition of Cyber ethics would depend upon a new definition of cyber. Let us try a new definition of cyber. Cyber<sup>12</sup> can be defined as: *an idealized free and unrestricted realm of spatial, conceptual, and spatio-conceptual hybrid activity, that arises in response to the adoption of machine assumptions – such as quantification, repetition, binary decision, and stepwise procedure – actualized as complex physical technology, in order to gain fine control of experience*.

The breaking out of cyber-ness – in the sense of growth – can be characterized as the ethically good aspect, or tendency, relatively, in response to machine thinking which is a relatively devaluative and unethical tendency of action.<sup>13</sup> As I have suggested through this paper, the vision of cyber ethics thus far, often unconsciously, has been to *correct for* – note the *for* – the devaluations built unreflectively into cyber-related technology. This cannot work. The devaluative assumptions actualized in the technologies in question work unceasingly once embedded, devaluating whatever is fashioned through them.

For example, the devaluative repetition that the architecture of the computer actualizes, finds its way into whatever the computer is used to help create, whether the computer be linked to physical mass manufacturing, or be used to access cyber and flood it with spam, propagate repetitive ‘likes’ for online content, etc. The computer comes to be used for such devaluations because the assumptions behind its design both facilitate and promulgate them.<sup>14</sup> To not use a computer according to the assumptions embedded in it takes a countervailing effort, which typically fails more often than it succeeds. In this sense the computer-related unethical *is* done because it *can* be done, the nature of the computer promotes and urges us to do it.

To be successful a future cyber ethics cannot merely *correct for* the devaluation of machine control thinking after the fact. It will have to *correct* machine control thinking in itself. Thus, in conjunction with the above definition, we might redefine Cyber Ethics as: *the reflective study and application of principles and concepts that can consistently engage machine control thinking assumptions applied in the physio-technological realm and its cyber by-product, so as to transform and expand those assumptions toward a more consistently valuative engagement of experience*.

In other words, the goal of a consistent future cyber ethics would be to recreate and create technology that is increasingly and relatively ethical, inherently, based upon its conception and developmental process. To pass on to analogy, current cyber ethics is attempting to eliminate weeds. Cutting the weeds after the fact is a hopeless task, as (Thomas & Ahyick, 2010) among others, have illustrated in research showing that ethical awareness does not substantially change behaviour in relation to fully fledged computer technologies. Nor can the weeds be squeezed out by other varieties of weeds, i.e. all those variations of control assumptions – regulations, committees, codes, laws, etc. – which accompany negative ethical approaches. Instead, a consistent future cyber ethics will refashion the very seed from which those weeds grow, so that it grows into something better.

<sup>12</sup> It need not be called *cyber*. The name is indifferent to the concept of a free beyond arising from the control assumptions of machine technology, except in the sense of its historic use thus far in relation to the development of the latter.

<sup>13</sup> For a fuller account of devaluation as an active ethical stance toward experience, see (Anderson, 2019).

<sup>14</sup> A computer can be defined along these lines as: *the tool which copies, repeats, quantifies, stores (repeats in time), sends instructions (causes a locus of experience beyond itself to replicate an activity), proceeds stepwise, etc. etc.* (Gray, 1999) gives a good overview of the development and dream of the thinkers who promoted and actualized the machine control assumptions behind computers.

Successful cyber ethics will, in a sense, remove the need for cyber. Or rather it will bring the value of the relatively good conceptualized as cyber (e.g. freedom from control, variation of experience to be interpreted) into the physio-technical realm of machine thinking, transforming the latter.

### **1.2 Suggestions toward a Positive Mode of Cyber Ethics**

Having attempted to redefine both the notion of cyber and cyber ethics relative to machine control thinking, can we offer some suggestions as to how to begin engaging more positive cyber ethics that could transform the root of the problem, i.e., the very assumptions that are being built into computer technology?

A promising start would be to turn to a more positive ethical mode as opposed to a control-centered mode of ethics, since, as argued, the context of the technology in question is not likely to respond to tendencies that emulate those very tendencies which cause the problem. Among others, in this context, a positive ethical mode:

- describes what one ought to do in terms of value because value – but not values – is general to all ethical understandings,
- actively builds value, through active suggestion and guidance from within ground-level contexts, and yet not merely locally but with an eye to being as generally consistent as possible,
- assumes that no real ethical advance will be made unless sources of value building (e.g. humans) act expansively, i.e. they are not forced into acting but are becoming sources of ethical betterment which then radiates outward from them,
- strives to build consistency in explanations of various active modes of creating value,
- strives to interpret various values in play in terms of more general consistent understandings of value<sup>15</sup>,
- forgoes control assumptions as a working position, e.g. forgoes links to law and regulation, in favor of peaceable but arm's length coexistence with the latter whenever possible<sup>16</sup>,
- recognizes that the physio-technological construct – the 'gateway' to cyber – is not neutral but on balance is based upon ethically devaluative and inconsistent assumptions,
- reflects upon and makes suggestions for the gradual transformation of physio-technological constructs,
- recognizes that the 'real' and cyber worlds are not separate, e.g. as in (Haigh and Jones, 2007) and (Aderibigbe, 2021), but that certain approaches to the former give rise to the latter and that nonetheless the devaluations of the 'real' world bleed into the cyber world.

The positive and active ethical mode of approach, applicable to any context of experience, should be combined with the *contexts* of cyber technological experience. In other words, our interest is best placed in the specific contexts of that experience, while looking to the generalities of the positive ethical mode as a rough guide and expanding upon them. In that process, more specific transformations will disclose themselves and can then be applied and generalized. They will include various angles of ethical transformation such as the following, with suggestions for engaging each theme first through a mode of reflection and observation and then through a mode of active and constructive guidance.

<sup>15</sup> Approaches to this include that of E.S. Brightman (1933).

<sup>16</sup> For more on this approach to ethics and law, see Anderson (2022).



**Reflecting ethically upon the ways in which the cyber world has a rebound effect ethically upon the ‘real’ world through the gateway of computer technology:**

- How does the notion that actions within cyber have no devaluative consequences with respect to repetition, i.e. ‘an unlimited space to fill,’ normalize repetitive commodification in the ‘real’ world? Devise qualitative actions within cyber with respect to our creations, with which to begin reversing the commodifying effect.

- How does cyber devaluation normalize ‘real’ world devaluation in terms of our earthly environment? Alter or adapt the computer designs stemming from machine control thinking by observing those patterns in nature which facilitate the more valuative co-existences in nature.

- How does cyber devaluation in terms of the quantity of acquaintances rebound upon ‘real’ world social ties, e.g. devaluing friendship, family ties, and the civilities of everyday physical interaction? Devise forms of non-quantitative sociality within cyber which can serve as models and improve linkages to ‘real’ world social bonds.

- How is the ease of setting up cyber gathering spaces for communal interaction hijacked by certain groups, e.g. Big Tech or extremist groups, so as to rebound upon ‘real’ world gatherings? Devise cyber gathering places that promote quality of interaction over quantity. Devise techniques for guiding users in cyber so as to defend against the influence of the respective bad actors.

**Reflecting ethically upon the birth processes of computer technology in terms of value:**

- Why are specific components within computer systems designed the way they are? Design them differently without machine control thinking.

- Where did these design ideas for ‘hardware’ come from? Locate the devaluative assumptions within them and replace them with more valuative ethical assumptions.

- What assumptions about value lie behind the various logics drawn upon in contemporary software? Construct alternatives to binary decision assumptions as a new base for software.

**Reflecting ethically upon those efforts which justify the devaluative engagements of and consequences upon the physical human body by simply accepting the separation of the real and cyber worlds:**

- In what ways are arbitrary boundaries assumed and created between degrees of machine control thinking? (Mazis, 2006), is a good example of reflection on this issue. Deliberately move our technologies away from machine control thinking by re-visiting and re-applying the qualitative aspects of our bodily physicality along with those of other creatures.

- What interpretive linkages between the ‘gateways’ to the cyber world and the cyber world have we been conditioned to deliberately forget (e.g. the narrowings of the keyboard, the cell phone screen, and many others) so as to physically devalue ourselves? Redesign these ‘shackles’ in ways that break out of quantity, i.e. in ways that offer qualities of experience more tempting than the repetitive and debilitating constrictions of quantity we have become used to.

- What parallels are there between the ‘cybers’ that have been imagined relative to the restrictions that nature imposes on our physical bodies and that which we have now developed deliberately ourselves? Using the knowledge of how the human body has evolved in context to overcome such restrictions, put it to use in designing technologies that will have more qualitative tending relationships with our bodies.

Of course, these suggestions are offered with the awareness that there are large counter forces at work, e.g. the habits of machine thinking related to capitalist economic models and industrialization and enterprise, epitomized in Big Tech, which takes full advantage of the devaluative tendencies of machine control assumptions. The influence of the latter goes beyond our computer-based technologies. Those of

good faith are not likely to beat such relatively devaluative forces at their own game. There is no easy way forward, except to meet the moves of these forces with sustained, consistent, and valuative redevelopment of our technologies under a positive outlook. Cyber ethics will have to come to reflect upon and come to terms with how the technology that gives rise to cyber is inherently, though relatively unethical. It will then have to suggest how to transform the machine control assumptions and create an alternative.

## 6. Conclusion

Maner (1996), Moor, and others, were right to view computer ethics as a special and unique field, but they did not locate the source of that uniqueness. The uniqueness stems from assumptions about the control of experience which have given rise to computers. Those assumptions have resulted in other technologies, but none yet as complex as computers. Computers are technologies that are not merely constructions whose design embeds such assumptions. They are technologies that propagate further designs based on those assumptions. In effect, computers are *the tool that replicates themselves and everything they touch, perniciously*.

I have argued in various ways that the notion and actuality of *cyber* stems from the individual and social intuition of this devaluative character in computer technology. The tensions in the emphasis by various thinkers in the history of cyber ethics illustrate this. Relatively contemporary accounts of cyber ethics still revolve around these tensions. The result is a tendency to offer ethical solutions that attempt to reconcile the freedom sought in cyber with the conditions – the design assumptions of the computer – that created the need for cyber. Typically, these advocate exporting control assumptions of the physio-technological realm into the free and virtual world of cyber: in-laws, codes, regulations, etc. while tying these, mistakenly, into ethics, so as to give the latter a decidedly negative and regulatory coloring.

This is not only an effort after the fact and too late but also doomed to failure. Proceeding in the negative mode, cyber ethics cannot achieve more than ethics achieves in the physical world in the same mode. Insofar as control does not work in the physical world – e.g. in laws and regulations – it will not work in the cyber realm. Where it does work, the advantages of the cyber realm are simply given up in favor of the overlaying of the control assumptions of the physical realm. And this overlaying of control assumptions is increasing rapidly in cyber. The end result will be a ‘cyber of cyber’ – though it may not go under that name – which is felt to be necessary in order to escape from machine control assumptions embedded virtually.

Thus, it is not enough to argue, as (Fuchs et al., 2009) do, that cyber ethics must concentrate on a notion of values that is essentially social and human-centered, and that technology is neutral in itself. Consistent future cyber ethics will need to gain a consistent understanding of value in order to assess the structures that form the gateway to cyber. The turn to a positive and active ethical mode could then be fruitfully applied to transforming those structures in various ways.

To advance we will have to unmake what we have made and rebuild it differently without imbedding the devaluations of machine control thinking. This will involve making use of the rebound effects of cyber upon the physio-technological realm, redesigning the foundations of computer architecture and logic, and returning to listening to the human body so as to rebuild its relation to a transformed computer technology consistently.

At its best cyber ethics could ultimately be an exciting experiment in creating a new realm, a deliberate expansion but not an escapist response, where the assumptions of machine control are gradually abandoned. This is its advantage, that it can serve as a testing ground for a higher level of ethical advancement.

## REFERENCES

Aderibigbe, N. A. (2021). Synopsis on Cybernetics' Behavior: A literature review. *Inkanyiso: Journal of Humanities and Social Sciences*, 13 (2), 273-290.

**Alhassan, J.K. et al. (2019).** “A Framework for Cyber Ethics and Professional Responsibility in Computing.” In Sengodan, T. et al. (Eds.) *Advances in Electrical and Computer Technologies*, (672). Singapore: Springer. [https://doi.org/10.1007/978-981-15-5558-9\\_28](https://doi.org/10.1007/978-981-15-5558-9_28)

**American Institute of Electrical Engineers Committee on Code of Ethics (1907).** Proposed Code of Ethics. *Transactions of the American Institute of Electrical Engineers*, 26(2), 1421-1425. <https://doi.org/10.1109/T-AIEE.1907.4764869>

**Anderson, M. M. & Fort, K. (2022).** Human Where? A New Scale Defining Human Involvement in Technology Communities from an Ethical Standpoint. *IRIE, Journal of the International Center for Information Ethics*, 31 (1), <https://doi.org/10.29173/irie477>.

**Anderson, M. M. (2019).** *Hyperthematics: The Logic of Value*. New York. Suny Press.

**Anderson, M. M. (2022).** “Some Ethical Reflections on the EU AI Act,” In *Imagining the AI Landscape after the AI Act. CEUR Workshop Proceedings. 3221 (Sept.)*. <http://ceur-ws.org/Vol-3221/>

**Brightman, E. S. (1933).** *Moral Laws*. New York: Abingdon.

**Bynum, T. W. (2000).** The Foundation of Computer Ethics. *ACM SIGCAS Computers and Society*, 30(2), 6-13. <https://doi.org/10.1145/572230.572231>

**Campbell-Kelly, M. et al. (2018).** *Computer: A History of the Information Machine*. New York: Routledge.

**Cyber 70 Computer Systems Product Announcements. (1971).** *Control Data Corporation*. [http://www.bitsavers.org/pdf/cdc/cyber/cyber\\_70/Cyber70\\_ProductAnnouncement.pdf](http://www.bitsavers.org/pdf/cdc/cyber/cyber_70/Cyber70_ProductAnnouncement.pdf)

**Fuchs, C., Bichler, R.M., & Raffl, C. (2009).** Cyberethics and Co-operation in the Information Society. *Science and Engineering Ethics*, 15, 447-466.

**Fogel, S. (1989).** Panic Compendiums. *Border/Lines*, (17).

**Goodwin, C. D. & Rogers, A. (1997).** “Cyberpunk and Chicago. The State of the History of Economics.” In James P. Henderson (Ed.), *Proceedings of the History of Economics Society*. New York: Routledge.

**Gotterbarn, D., Miller, K., & Rogerson, S. (1999).** Software Engineering Code of Ethics is Approved. *Communications of the ACM*, 42 (10).

**Gray, J. (1999).** “What Next? A Dozen Information-Technology Research Goals.” *Technical Report MS-TR-99-50*. Redmond. VA: Microsoft.

**Guerry, B. (2001).** Logiciel libre et innovation technique. [https://bzg.fr/img/logiciel\\_libre\\_innovation\\_technique\\_bastien\\_guerry.pdf](https://bzg.fr/img/logiciel_libre_innovation_technique_bastien_guerry.pdf)

**Haigh, C., & Jones, N. (2007).** Techno-Research and Cyber-Ethics: Challenges for Ethics Committees. *Research Ethics*, 3(3), 80–83. <https://doi.org/10.1177/174701610700300304>

**Hahanov, V. et al. (2011).** Cybercomputer for information space analysis. *9th East-West Design & Test Symposium (EWDTS)*, 66–71, doi: 10.1109/EWDTS.2011.6116416.

**Johnson, D.G. (1997).** Ethics online. *Communications of the ACM*, 40 (1, Jan.), 60-65. <https://doi.org/10.1145/242857.242875>

**Liddell, H. G. & Scott, R. & Drisler, H. (1883).** *A Greek English Lexicon*. New York: Harper.

**Loomis, B. (2015).** “1900-1930: The years of driving dangerously.” *Detroit News*. April 26.

**Maner, W. (1996).** Is Computer Ethics Unique? *Science and Engineering Ethics*, 2(2), 137-154.

**Mazis, G. A. (2008).** *Humans, Animals, Machines: Blurring Boundaries*. New York: SUNY.

**Moor, J.H. (1985).** What Is Computer Ethics?, *Metaphilosophy*, 16(4).

**New Products. (1984).** *Antic Magazine. The International Atari*. 2(12).

**Nooney, L. (2021).** How the Personal Computer Broke the Human Body. *Vice. (May)*. <https://www.vice.com/en/article/y3dda7/how-the-personal-computer-broke-the-human-body>

**Pusey, P., & Sadara, W. (2011).** Cyberethics, Cybersafety, and Cybersecurity, *Journal of Digital Learning in Teacher Education*, 28, 82-85.

**Sætra H.S., Danaher, J., (2022).** To Each Technology Its Own Ethics: The Problem of Ethical Proliferation, *Philosophy & Technology*, 35(93). <https://doi.org/10.1007/s13347-022-00591-7>

**Sakka, G. & Spyrou, I. (2015).** “CyberEthics Case Study.” In *Human Right and Ethics: Concepts, Methodologies, Tools and Applications*. Hershey PA: Information Science Global.

**Spinello, R.A. (2017).** *Cyberethics: Morality and Law in Cyberspace*. 6<sup>th</sup> Edition. Boston: Jones & Bartlett Learning.

**Sedlet, S.M., & Dust, J. (1981).** "Linking a Pascal Microengine to a Cyber 170" in *Byte Magazine*, 6(11). <https://archive.org/details/byte-magazine-1981-11/page/n481/mode/2up?q=cyber>

**Tavani, H.T. (2015).** *Ethics and Technology: Controversies, Questions, and Strategies for Ethical Computing*. 5<sup>th</sup> Edition. Wiley.

**Thomas, T., & Ahyick, M. (2010).** Can We Help Information Systems' Students Improve Their Ethical Decision Making, *Interdisciplinary Journal of Information, Knowledge, and Management*, 5, 209-224.

**Quina, K., & Miller, D. L. (2000).** "Feminist Cyberethics." In M. M. Brabeck (Ed.), *Practicing feminist ethics in psychology*, American Psychological Association. 143-165. <https://doi.org/10.1037/10343-007>

**Wiener, N. (1950).** *The Human Use of Human Beings*. Boston: Houghton Mifflin.

**Zhang, H. (2022).** "Report from the First Workshop on Cyber Ethics in Platial Research." In *Third International Symposium on Platial Information Science (PLATIAL'21)*, Enschede, the Netherlands. <https://doi.org/10.5281/zenodo.6413003>