Civilizing New Forms of Artificial Intelligence: A Review Essay of "The Impact of Ambient Intelligence Technologies on Individuals, Society and Warfare"

Mark R. Hagerott, Ph.D.
North Dakota University System Chancellor

Keywords: *A.I., AmI. Artificial Intelligence, surveillance, robotics, warfare, social change*

The essay, "The Impact of Ambient Intelligence Technologies on Individuals, Society and Warfare," (IAITISW) offers a thoughtful, wide ranging look at the emerging intersection of multiple sensory and computational technologies that together form what is becoming known as Ambient Intelligence (AmI). The authors are commended for focusing on this emerging socio-technical phenomenon, as the effect of this technological nexus will be far reaching, manifest at the level of the individual and larger society. In perhaps the most profound decisions a society will make, AmI may influence "life and death" calculations, and may well determine who wins and who loses the wars of the future.

Before proceeding further, it may be helpful to restate the authors definition of AmI:

> [E]xtends advances in computing power, artificial intelligence and distributed sensor networks...AmI technologies permeate the environment with intelligence and create a symbiotic relationship between humans and systems...AmI is comprised of networks of intelligent agents that are sensitive, responsive and adaptive to changes (e.g. temperature, lighting, etc.)p in the environment and to personal preferences...These collaborative networks of intelligent agents evaluate information, communicate with each other, as well as develop plans and make decisions (IAITISW).

As can be seen in the definition, Ambient Intelligence technologies are derivative of scores of other systems or 'systems of systems.' Given the importance of and unintended consequences associated with the growing intersection of myriad systems, this analysis of AmI may be a forerunner of more essays to come on this subject. While much of the literature surrounding IT innovation is technical in nature, this work goes farther and ponders the socio-technical-military implications of intersection and emergence.

The essay is structured around three concerns: AmI and the private citizen (a person's health care is offered as an example); AmI and war of the future (for example, the human struggle to perceive and control the battle space as intelligent machines proliferate); and the implications of AmI for society at large (for example, pondering the question what will freedom and privacy mean in an environment densely populated by AmI technologies).

One of the many strengths of IAITISW's essay is the ability of the authors to tackle a complex, emerging phenomenon, and provide illustrative examples of this emergence. The authors sketch out the possibilities for AmI to solve problems of elderly persons, many of whom live in isolation. The AmI now

coming into focus may be just the early manifestation of technologies that increase the health and wellness of the elderly. For example, the authors describe recent efforts to make cities and homes "smart", better able to provide greater health and security for vulnerable populations. They ask us to consider China's "Digital City" effort:

> Today, there are more than 200 million people above the age of 60 years of age...Thus, there is a need for China to implement smart digital cities as a potential solution. Smart cities will be built with smart homes. This includes a multidisciplinary approach to monitor health, food, lifestyle, wellness and social aspects of daily life, built into the design. Medical monitoring of health will be the overlay of each of these designs aimed at addressing the elder care issue.

While the elder care example seems to portend many positive outcomes, the military section of IAITISW is less sanguine. Many readers, even those without military experience, can imagine examples wherein AmI technologies might pose a challenge to the battlefield commander and the human imperative to comply with the 'laws of war'. As has been demonstrated recently in the battlefields of Iraq, Syria, and Afghanistan, scores of semi-autonomous machines are engaged in combat operations. What is less obvious to the general public is the existence of networks of sensors that collect information, and feed this information to high powered computer systems that do the 'thinking' about the data. The rising number of netted machines, the volumes of data, and the ever increasing speed of data analytics have combined to push warfare in the direction of what the authors describe: the emergence of Artificial Intelligence (AI) and its close cousin, AmI. The technical challenges of controlling such a complex machine system are daunting.

But rightly, IAITISW's authors express concern less with the technical challenge of assembling such a mass of machinery, than with the ethical implications of increasingly robotic warfare, connected to and informed by AmI technologies. Thankfully, these capabilities are just in their early stage; we haven't seen the full effect of AI and AmI. Thus, policy makers and the broader citizenry need not worry about these sci-fi military futures...or do they?

This essay is heady stuff. Readers may feel weighed down. And readers can perhaps ask: why bother ourselves with thinking about such problems now, why not weigh in later, after the technologies and usage patterns mature, and robotic warfare, AI and ubiquitous AmI become a reality? History of technology with its many examples of "technology out of control", would argue for early thinking and earlier intervention. If policy makers and larger society wait too long to engage issues of technological emergence, patterns of usage and development often "lock in" precluding societal intervention later. History has shown (see the theories of Paul David (QWERTY) regarding information systems, and Thomas Hughes' work on power systems and Donald McKenzie on the nuclear arms race) that emergent technological systems have a tendency to gain momentum, and usage patterns "lock in" with adverse consequences for successive generations saddled with suboptimal outcomes. For example, the development of nuclear weapons was allowed to proceed unchecked in the 1950s and soon developed a dangerous momentum that contributed to the near incineration of the world in 1962. Quickly after the Cuban Nuclear Missile Crisis restrictive controls were put in place, producing within several decades treaties that eliminated masses of

these dangerous machines. More recently, the momentum of early, flawed nuclear power plant designs came to dominate the Japanese energy industry, a momentum that was stopped only in the catastrophic tsunami of 2011 which left four reactors smoldering and large areas of country uninhabitable. Both problems were the consequence of technological "lock in," which came about when prior generations failed to intervene early when smoother, less dangerous and disruptive policy change would have been possible. By waiting so long, a window had closed, thus changing the trajectory in technological development required disaster or near disaster in order to gather the political and social consensus for new policies.

So, one might ask: is the window closing again? We are on the cusp of the emergence of a massive new set of technologies, AmI. We must grapple with the implications of this "technological progress" and try to understand the nature of the problems and challenges with these technologies. In some sense, we as society have been here before. Today's problem is akin to what our 19th century leaders faced when grappling with the Industrial Revolution: how to control and shape emergent technologies such that they ultimately serve and provide for the public good. In the phraseology of the especially insightful historian of that period, John Kasson: how did our forefathers succeed in "civilizing the machine".

Our great-grandparents "civilized" Industrial Revolution technologies by the creation of new laws and multiple regulatory agencies (e.g., Food and Drug Agency; the Environmental Protection Agency). Their success can yield some important analogies and insights germane to the problems of AmI. However, there exist some differences between *Industrial* Revolution technologies and *Information* Revolution technologies that may make 'civilizing' efforts particularly challenging.

First, unlike Industrial Age technologies such as the speeding locomotive, roaring jet aircraft, or teeming masses of automobiles belching exhaust on a cold winter day, this time around it is more difficult for a human to see and perceive many of the side effects of emerging AmI machines.

A second concern relates to the susceptibility of AmI to hacking combined with the invisibility of much AmI. Might such a dualistic nature of AmI create a threat vector through which hackers can obscure the negative effects of AmI while they threaten the security of the human who is in proximity of the AmI? For example, the authors point to computer Intrusion Protection/Detection Systems (IPS/IDS) as examples of important and emergent AmI (see IAITISW). These forms of AmI work outside and beyond the human senses, rapidly perceiving and some cases blunting the attacks of threatening computer code. But who among us would know if the IPS/IDS was itself hacked, and working against the human's best interests? For example, the infamous STUXNET attack was never perceived by either Iranian IPS/IDS systems nor the human operators, yet the attack yielded substantial damage to three dimensional, real machines.

Thirdly, these machines are increasingly "intelligent", and some are designed to learn. Society acting through wise human operators and ever vigilant government regulators can monitor these learning machines and thus intervene to control these intelligent machines, so far. But these machines will continue to learn and the question remains unanswered: what will they learn in the future? Recall that recently, Microsoft programmed a social media algorithm to observe, learn, and modify its own behavior based upon interactions on the internet. In less than a

day the MSFT bot was learning the wrong things and taking on the language of neo-Nazis it had interacted with on the internet. A similar possibility seems likely to confront intelligent, AmI learning programs. But even if AmI intelligent algorithms are not purposely misled or hacked, the question remains as to how AmI would learn ethics and norms congruent with our society. Moreover, if AmI algorithms start to learn faster than human operators and regulators can learn, which I suspect will be the case, how can we ensure human control of the machine let alone human shaping of the ethics and norms the machine will adopt?

The authors have produced a wonderfully thoughtful and future looking essay. What follows are some suggestions for future work and reading related to this topic. We need to examine again the trajectory of AmI technology, looking back before the "start date" of 1999. It might be argued that our society and our IT industry have been assembling the building blocks of AmI for decades. It may be that only in the past two decades has the momentum toward powerful and ubiquitous machines become emergent so as to allow us to identify such a thing as Ambient Intelligence[1].

Some writers in the field endorse the view that AmI may benefit the military by reducing personnel costs (IAITISW). I encourage readers to question the assumptions underlying such a future of cost savings. If we include the long term cyber security costs involved in AmI, both in securing the supply chain but also in the continuous monitoring and repair of cyber vulnerabilities of the supporting algorithms and network connections, the costs might be far higher than is the case today with more human intensive systems.

The IAITISW authors introduce a fascinating possibility: that AmI machines may begin to practice "Deception". This possibility is worth exploring further. AmI is uniquely positioned to "check mate" all other systems because of their position in the initial phases of any human-machine decision cycle: AmI are crucial to a correct "sensing" the environment. All the physical weapons and virtual weapons such as cyber security software would be rendered ineffective (or even traitorous?) if such systems were deceived as to the reality they confront. So, how do we protect against being deceived by our machines? Perhaps laws that limit the speed and sophistication of such 'systems of systems?'

A last couple suggestions regarding additional reading. For the benefit of readers interested in better understanding possible technological futures, I would read Kevin Kelly's "What Technology Wants" and David Egger's "The Circle." In response to the increasing automation of weaponry, several arms control groups have come together to advocate for greater human intervention and monitoring, what is termed "Meaningful Human Control." For more on this issue, I would direct readers to the United Nations Convention on Certain Conventional Weapons (UN CCW) online resources, groups found at ICRAC.org, and the International Red Cross. For additional history on the evolution of technology, consider Paul David's seminal essay explaining the origins of QWERTY; Neil Postman's, "Technopoly"; James Beniger's, "The Control Revolution." Lastly, one of my favorites, John Kasson's, "Civilizing the Machine."

Concluding Comments

IAITISW's authors are focused on a critically important nexus of technologies,

[1] AmBIntell is now rapidly entering public mind in form of Amazon Alexa.

Ambient Intelligence. There is no stopping the continuing emergence of AmI; the emergence of A.I. may be, as Kevin Kelly argues, a "force of nature." But a "force of nature" can be shaped and channeled. Now is the time to shape the future of this technology; to draw policy and ethical contours for the future. Why? Because technologies have an historical tendency of gaining momentum, and it is far easier to maximize social good if thoughtful leaders engage early. To be sure, there are many positives of this technology, from the formation of new industries, new jobs, and the increased possibility that wars of the future may result in fewer humans at risk. But there are many down sides. Hopefully essays on this topic will help raise awareness of the pitfalls and prospects of a technology that is sure to shape much of how we live, work, and how our military may fight in the coming decades.

Dr. Mark Hagerott *is Chancellor of the North Dakota University System, and concurrently holds a joint appointment (non-tenured) in the NDSU department of History, Philosophy, and Religious Studies and a Cyber Fellowship (NR) at the New America Foundation. Previously he served as a member of the Defense Science Board Summer of 2015 study of autonomous machines, in the history department faculty at Annapolis, and as the Deputy Director of the U.S. Naval Academy Cyber Center.*

Earlier in his career, Hagerott served as a naval nuclear engineer, naval tactical data network manager, and combat systems engineer of the highly automated AEGIS weapons system. He is published in International Journal of Critical Infrastructure Protection, Cyber Security Policy and Research Institute, National Academy of Sciences (Issues.org), Foreign Policy Magazine and Combat Studies Institute. He has published book chapters on changing technology and military workforce development, and was awarded the John D. Hayes Fellowship in Naval History in 2007. In 2014 he presented before the Geneva Convention conference on the ethics and operational dangers of lethal robotics. Hagerott holds a Master's degree from Oxford University in politics and economics (where he was a Rhodes Scholar) and a PhD in the history of technology from the University of Maryland.