The Impact of Ambient Intelligence Technologies on Individuals, Society and Warfare

"The real problem is not whether machines think but whether men do" B.F. Skinner

Yvonne R. Masakowski, Ph.D., Jason S. Smythe, M.A., & Thomas E. Creely, Ph.D.

Abstract

Advances in Ambient Intelligence (AmI) technologies have significant implications for individuals, society and warfare. This paper examines ethical challenges associated with the development of the emerging discipline of Ambient Intelligence technologies. It is argued that Ambient Intelligence technologies, while providing support for many aspects of everyday life and well-being, may also present increased privacy risks and potential risks to national security.

Keywords: *Ambient Intelligence, Ubiquitous Computing, Intelligent User Interfaces, Cyber Crime, Ethics, Freedom, Privacy*

Introduction: The emergence of Ambient Intelligence Technologies

The 21st Century has seen the emergence of numerous advanced technologies such as personal computers, cell phone technology, cognitive robotics, artificial intelligence, and autonomous, unmanned systems that collaborate with humans and other systems. This vision of the future was inspired by the Philips Company (1999) which was the first organization to predict that a distributed network of intelligent devices would support humans with communication, information and entertainment. Ambient Intelligence (AmI) has been characterized by the integration of pervasive computing power and intuitive interface designs. One of the key characteristics in an Ambient Intelligence environment is that AmI technologies must be context aware of the environment in which they are being used. AmI technology embedded in the environment, in combination with wireless communication, has the capacity to identify an individual's geolocation to deliver context-driven personalized information in a natural and intuitive manner. Ambient intelligence may be integrated into robotics, autonomous unmanned systems and integrated with distributed sensor networks embedded in our environments.

Advances in computing power combined with an increase in the capabilities of AmI will transform the ways in which we live, work and maintain security on a global scale. Technology breakthroughs via AmI will influence and shape the ways in which we interact with the environment. AmI systems will support adaptive Intelligent User Interfaces (IUI) that is proactive vs passive.

AmI facilitates the dissemination of information on a global scale which presents both advantages and challenges for the future global security environment. For the individual, this technology provides a means of facilitating enhanced health care management but also raises concerns regarding our personal freedom and privacy issues. For the warfighter, it provides a means of managing the battlespace from a centralized command via the network. For the adversary, it provides the capability to conduct operations in a decentralized manner. For society, it presents challenges to personal privacy and freedom.

AmI Technology

AmI extends advances in computing power, artificial intelligence and distributed sensor networks that have revolutionized the way we live by providing " a digital environment that proactively, but sensibly, supports people in their daily lives," (Cook, 2009). AmI technologies permeate the environment with intelligence and create a symbiotic relationship between humans and systems that may be tailored and personalized to meet the individual's needs.

AmI is comprised of networks of intelligent agents that are sensitive, responsive and adaptive to changes (e.g. temperature, lighting, etc.) in the environment and to personal preferences. Intelligent agents are autonomous, computer generated systems that communicate and collaborate with each other (Dilek, Cakir & Aydin, 2015). These collaborative networks of intelligent agents evaluate information, communicate with each other, as well as develop plans and make decisions. Such networks are often used in security systems wherein complex, adaptive multi-agent systems provide a means of preserving information, as well as protecting the system from attacks.

The dynamic nature of the information environment requires a network that is robust and capable of assessing and prioritizing information required by the user in a timely manner. AmI technologies integrate components of human intelligence such as language, speech recognition, image recognition and knowledge as part of the intelligent agent network. Thus, intelligent agent architectures serve as the cognitive components of a multi-agent intelligent agent network system. These networks of intelligent agents are adaptive, formulate and evaluate hypotheses, communicate and collaborate with other agents in the network to develop plans and make decisions.

Biological computational models are often designed for intrusion detection as they provide an adaptive response to intrusion detection. Experiments have shown the benefits of bio-inspired systems with fuzzy detection systems in improving detection precision (Pei and Song, 2008). One of the main advantages of fuzzy rule-based systems is the flexibility in dealing with subjective and objective knowledge and vague concepts (Masakowski & Grasso, 2012). Genetic algorithms model the natural selection process using a machine learning approach. This evolutionary biological system integrates a rule-based approach to develop adaptive responses to potential security threats (Kim, Yang & Sim, 2004). The Artificial Immune System (AIS) computational model also mimics the biological immune response thereby providing an adaptive response for detecting and defending against potential attacks (Qiang &Yiqian, 2010). AIS systems, similar to the natural immune system, are designed to detect intrusions and maintain homeostasis in the system and thereby play a pivotal role in cyber security.

Advances in the development of bio-inspired computational models serve as an example of the flexibility and adaptability of intelligent systems that are robust enough to counter cyberattacks. Future systems must be designed to anticipate the potential threat as well as monitor detect and defend against it. Such systems must be proactive and designed from cognition-centric perspective vs the human-centric designs of traditional systems (Masakowski, 2008). That is, future AmI systems must be able to anticipate and perceive potential threats and opportunities for the individual and anticipate what the individual will think or want to do. Systems will need to recognize multiple users, and learn from their behaviours and interactions, as well as leverage information from their environment to anticipate their needs.

For the warfighter, AmI intelligent

agent networks must be designed to address questions in anticipation of an event from an adversary's perspective. The AmI system would have to posit hypotheses related to potential paths of intrusion, and potential security threats. Namely, what strategies might adversaries employ to achieve their objectives? How does their social network interact? How can the adaptive AmI network anticipate the threat, learn the adversaries' strategies, and develop proactive plans to effectively deter and defend against such threats? The digital "Butler" of the future may also be the future "Security Guard" for all networks.

Pervasive computing affords AmI technologies the capacity to be "context aware" and capable of adapting to dynamic changes in the environment (Brey, 2005). These embedded systems are transparent to the individual user and are woven into the tapestry of everyday life in a seamless manner. Indeed, AmI technologies are proactive and anticipate what the user requires from the environment. This ability to perceive the environment (context aware) and the location of the individual as well as an awareness of the individual's preferences, provides the AmI system with the ability to perceive, evaluate and make decisions without human input (Brey, 2005). This capability serves as evidence of the need to employ cognition-centric design rather than the traditional human-centric approach. Indeed, cognition-centric design goes beyond traditional interface designs by providing an intuitive, adaptive system that is profiled to the individual's preferences and anticipates his needs and preferences (Masakowski, 2008).

Today, we see evidence of AmI technology at work in our daily email as Amazon.com forwards recommendations for reading based on our book preferences and proactively prompts us regarding books we might find of interest in the future. Evidence suggests that AmI capitalizes on image recognition and visual search strategies. For example, there are pre-attentive processes and visual search strategies that humans employ (Triesman, et al, 1992) which may be modelled by the AmI network in anticipation of a human need and predict anticipated outcomes. For example, the information we seek is indicative of our intentions and may be combined with our specific profile within a context that would afford the intelligent agent network the means of making inferences about our situation and our intent. Specifically, AmI intelligent agent networks facilitate sensing, locating an individual and sense information from the environment which helps the AmI network to form perspectives and evaluate an individual's needs and intentions. Thus, these AmI intelligent networks have been designed to be aware of our identities, behavioural patterns, social networks, location, intentions, as well as anticipate and predict our future needs.

This represents a paradigm shift in information management wherein AmI technologies serve as a proactive computer technology which can be used to support public safety and security via embedded systems in the environment. As a benefit to society, the integration of AmI sensor networks within our everyday environment enables a system to provide security and safety for the public. For the individual, this transparent network provides critical support for everyday living and lifestyle management. For medical management, this system provides a means of monitoring senior health care and for those children in need of behavioural monitoring, such as Autism. (Georgia Tech
Research Institute, 2016)

For national security, this network provides a means of capturing and assessing accumulated data/information that may prove critical for national and global security. Certainly, the heightened awareness of

terrorist groups such as ISIS, et al. elevates the need to develop ubiquitous intelligence networks and surveillance technologies that can manage a vast network of information. Indeed, AmI technologies with its pervasive intelligent agent network provide a robust, adaptive and optimal means of combating cyberattacks and ensuring national and global security. In fact, there are digital cities being designed around the globe to take advantage of AmI technology.

Digital Cities and Security

The aim of AmI technologies is to make human life easier by creating an environment that is sensitive and responsive to our needs (Philips, 1999). To this end, AmI technologies have been embedded into the design of home environments to help humans live in a comfortable and safe environment. Originally, product designers and advertisers were among the first to capitalize on these innovations. Marketing firms quickly realized the advantage of personalizing ads to meet your specific desires and needs. Architects have extended the application of AmI to home design and have been designing digital cities around the globe. Each year, there is a digital city design competition (Wood, et al. 2015). Among the topics included in the design of the digital city is that of multi-jurisdictional cybersecurity. That is, cities are sharing the costs of cybersecurity with the advent of these technologies.

Digital cities are noted for their technological innovation which most often includes Cyber Security, Government transparency, Virtualization for data storage, Budget Management, Social Media, Mobile applications, Tracking technologies, Cloud Computing, Disaster Recovery and Geospatial mapping. Each of these technologies is aimed at supporting and managing the city and providing security for its citizenry. Each city recognizes the value of the technology to support their region and empower their leaders to be more effective in managing their cities.

Indeed, these technologies are aimed at bridging the gap of its digital divide by using open data architecture to keep their city's data secure. Among the principal success stories is that of the city of Winston-Salem, N.C. which uses cloud services, mobile tracking systems, internal and external use of social media and a WinstonNet program aimed at keeping the community program open to the community. Philadelphia was the recent winner of the Digital City design competition and acknowledged that this technology will enhance their cybersecurity (Wood, et al. 2015). Transparency is the key ingredient to the digital city design! The system tells each city how it is doing from a security, financial and physical infrastructure perspective. It highlights the risks and vulnerabilities of the city, as well as facilitating communications among cities in the network. Using a mobile pavement tracking system the GIS-based and GPS-enabled mobile application can monitor the condition of roads and paving projects. Cybersecurity is ensured by developing a joint effort with neighbouring communities to monitor and ensure security. The digital city design effort is a global event.

China has seen an expansive growth of its aging population. Today, there are more than 200 million people above the age of 60 years of age. Given their mandate regarding limitations on children, the one child solution has given rise to an emerging medical management crisis for the increasing aging population. 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. Interactive healthcare will be ubiquitous! Further, many universities in the US are also exploring innovative solutions to home design aimed at supporting human needs and requirements. Among these, the Georgia Tech Research Institute has designed an "Aware Home" that provides a means of exploring the application of technologies to support senior citizens in home health monitoring and care (GTRI, 2016). The "Bespoke" home design of the future will be an extension of your individual daily needs to ensure that you have a quality of life and level of security that is specifically designed for you.

These technologies extend to the military and defence departments as well. The tactics of warfare are well established; what changes are the technologies engaged. Warfare evolves based on technological advances ranging from the first Gatling gun, the tank, the fixed–wing aircraft, the aircraft carrier, the nuclear powered submarine to the first autonomous, unmanned vehicle (UUV, UAV, and UGV). Autonomous, unmanned systems operate as a machine that can think, collaborate with other unmanned systems and perform programmed behaviours such as collecting data, imaging and tracking. This cognitive capacity enables distributed networks of autonomous, unmanned systems to collaborate and coordinate on a mission. Likewise, drones have demonstrated their role in precision strike missions. Robotics is commonly used in military operations to defuse IEDs. There are significant benefits for engaging unmanned systems, drones and robots to preserve human life in combat situations. However, the challenge comes in when we think of the ethical and moral implications of integrating these systems with artificial intelligence, i.e. a brain. Russia has recently announced its intent to develop combat robotic guards to become operational in 2017-2018 (Defense Update, 2016). While the research continues, the ethical implications for engaging in robotic warfare are not a remote possibility but rather close at hand. Robots coded with a set of objectives, devoid of social morals, values or conscience, and designed with a network of artificial intelligence may have grave implications for our future. The questions are what is our response to this development in warfare as a society? How will we address the ethical issues raised in this regard?

The advent of artificial intelligence is not a new issue. Rather, in the 21st century with the development of technological advances in computing power, sensor systems, it is clear that we are closer to developing an artificial intelligence equivalent to the human brain. Kurzweil points to the topic of achieving singularity with robotics (Kurzweil, 2006, 2014). What is new is the fact that as technology advances in designing robots with self-awareness, this creates the opportunity for machines to surpass human intelligence. Thus, Kurzweil predicts that machine intelligence will become more powerful than human intelligence. While current efforts in Artificial Intelligence (AI) are aimed at developing medical mediation of disease, seizures, paralysis, and cancer; this pathway of exploration also avails itself to exploring the effects of cell-to-cell communication in the brain as well as brain-to-brain communication to enhance our sensory capabilities.

Kevin Warwick, a Professor of Cybernetics in the UK has explored the effects of implanting a device to interact with the human nervous system and the brain (Edgar, 2014). Creating cyborgs that are equipped with wireless transmitters in their brain enables a new kind of command and control for the 21st Century and beyond. Robotics being designed for personal use is aimed at supporting individual medical needs but these same systems can be applied in

other ways.

The advent of drones in the US military demonstrates the impact of this technology. Precision strikes have become known as part of the American lexicon as we hear of drone strikes on the news. Indeed, the DARPA Challenge raises the bar on these technologies with its robotic champion prize each year. Hubo, this year's DARPA Champion, exhibited its dexterity in climbing stairs and extending its legs (Guizzo & Ackerman, 2015). Evidence of the benefit of ambient intelligence and autonomous systems was noted by the F-16 whose automatic system, sensing its relationship with the terrain, made a rapid manoeuver to prevent the jet from crashing. In this scenario, the pilot still maintained the ability to override the system; that may not be the case for the future.

Recently, Professor Arkin of Georgia Tech demonstrated that robots are capable of deceit (Arkin, 2012). This study demonstrated the robot's capacity for adaptive learning. This is significant in that it provides an illustration of the evolutionary learning capabilities that can be utilized by a robotic system. Namely, nature provides us with biological models for mimicry and deception that may be exploited in an autonomous, unmanned system and/or robotic algorithm. Thus, it is incumbent upon us to examine the ways in which technologies are being designed and integrate anti-deception intelligence into the design. This must be part of the original design and a sensor network that is sensitive to the effects of potential deception and mimicry. Deception built into the design of autonomous, unmanned systems (e.g. drones and/or robotics) may be our new vulnerability!

Ethics and Ambient Intelligence Technologies

While there are significant benefits for facilitating an easier lifestyle for the individual, AmI is a technology replete with ethical and privacy issues related to the management of personal information. Specifically, the ability to think and make decisions for oneself represents a sense of privacy that is fundamental to the American citizen. We concur with Tennenhouse's argument (Tennenhouse, 2000) that it is reasonable to delegate routine tasks to the level of a computing device; one should also consider the potential consequences for all decisions. We contend that humans have the responsibility to evaluate choices within the context of their own value-based beliefs. Although autonomous systems may support decision making, individuals must address the consequences for their decisions from cognitive and emotional perspectives. Decision making does not occur in a void but rather takes into consideration each of the costs and benefits as well as potential consequences for such choices. While some of these trade-offs may be modelled in an autonomous system, others may not. Further, decision making is a sign of independent thinking, personal choice, privacy and freedom. If a machine makes choices and decisions for an individual; then, the individual has yielded and lost their right of choice. Rather, they have surrendered their independence, privacy and individual freedom. Are we as a society willing to give up these rights?

Panopticon and Privacy

As AmI envelops the human experience, Philosopher Jeremy Bentham's Panopticon clearly comes into focus at a new level for surveillance. The optical system developed for prison behavioral control was "the" great innovation for "easy and effective exercise of power" (Foucault, 1977). Panopticon projects through AmI the power of the gaze into the intimacy of living and

thinking. Technology, such as AmI, is increasingly all-seeing as it is incrementally developed for the purposes of improving the human condition.

The gaze peers into the private lives of individuals to the extent that privacy boundaries are at least blurred if not erased. AmI homes can provide safety, comfort and economy on many levels (Cook, et. al., 2007). As with any technology, security, convenience, and efficiency come with tradeoffs, especially the loss of freedom.

Samuel Warren and Lewis Brandeis wrote the seminal law article on privacy stating, "Everyone has the right to be left alone…" (1890). Even in antiquity Cicero stated, "What more sacred, what more strongly guarded by every holy feeling, than a man's home?" Does AmI violate the sacredness of home? Privacy? Personhood? AmI is part of the transparent tapestry of our daily lives from which we may derive benefits regarding our health and security. The question is do we want to be left alone?

Ami collects, assimilates, analyzes and interprets some of the most sensitive information on a person's behavior – the result of conscious and unconscious thinking. AmI literature indicates that a person's decision-making would be critiqued, influenced and shared-control (Verbeek, 2009). It would also have the capacity to capture relationships of spouses, significant others and children. How would we set the boundaries of relationships? Would AmI intrude and interfere with relationships? Panopticon's power of the gaze was to control prisoners through the discipline of good behavior. The objective was for prisoners to be conscious of being monitored continuously around the clock as a means of maintaining discipline. AmI could infringe on one's sense of personal freedom and prove to be unnerving in your private home.

With the recent hacking of the "secure" U. S. Government Office of Personnel Management by the Chinese, troves of personal data were captured by the Chinese giving them significant political and military power. Edward Snowden easily downloaded some of the most secure intelligence data at the NSA. How could we, as a society and nation, ensure that we are safeguarded from intrusive AmI technologies that might monitor our thoughts and relationships? How would we safeguard ourselves against potential compromise based on data collected by AmI technologies?

Technology has become so pervasive that there is no privacy, as noted by tech industry CEO Scott McNealy, regarding the Internet. Evidence of hacking, cookies, malware and other information collecting technologies by commercial entities and governments demonstrate the impact of the Internet such that all information remains exposed. How do we ensure that code is written within an ethical standard to ensure privacy for the user?

How much freedom does one have if AmI learns our behaviors, speech patterns, language, gestures, moods, etc.? How will this awareness of each individual's behavioral patterns impact the AmI machine's decision-making? AmI literature reveals that this technology senses, measures, and analyzes habits and trends. This suggests that there will be a significant increase in the AmI system's capacity to extend its learning to anticipate individual and group behaviors over time. This raises a risk regarding the potential misinterpretation of intention on its part which may have dire consequences for the individual or for society as a whole.

AmI technology must be developed through the multidisciplinary lenses of ethics. We must address AmI technologies with a view toward preserving human rights and dignity. As AmI technology continues to move forward, we must be vigilant regarding the need to preserve individual freedoms,

privacy and ethical values. As AmI systems become more intelligent and capable of anticipating patterns of behavior and interactions with others, we may lose our sense of personal freedom and independence. The AmI system has the potential to erode each individual's rights of privacy, freedom and decision making.

The nature of AmI and the ethics imbued in it are relegated to the moral nature of those who program the machines. In their book, *Moral Machines*, Wallach and Allen (2009) discuss the implications of programming intelligent machines to make moral decisions. The very process of doing so requires the programmer to define morality and consequently provide it with limits and boundaries. These machines will be relegated to the moral capacity of their creator. Due to the inevitably flawed morality of human nature, these machines will be subjected to the same moral shortcomings. Intelligent technology cannot become more moral than what is programmed to be. How do we defend against such monitoring and control?

Giordano et al. (2015) present an argument regarding the potential pre-emptive nature of evaluating human behavior in anticipation of a negative event in society. Neuroscience and advances in neurotechnology may provide a means of evaluating individuals with a propensity for violence with the aim of preserving public safety. That said there are significant ethical and legal issues related to the misuse of these approaches. While there are significant advances in brain research and neurotechnology (e.g. SPECT, MRI, fMRI, etc.), there are ethical and moral issues related to predicting violent behavior similar to that found in the film M*inority Report*. The profound issue is that we assume that a neurotechnological approach will definitively establish a cause and effect relationship via inference from an individual's behavior, thoughts, propensities and form conclusions that may not only prove incorrect but may also prove harmful. Therefore, it is critical to evaluate the ethics of such an approach and address the considerable risks associated with such a practice.

Central to this argument, the issues of privacy, freedom of choice, decision making remain viable and ethically challenging. The question remains, how society maintains public safety and security while ensuring that this approach does not threaten our ethical values and rights to privacy and freedom.

Concluding Remarks

The convergence of Ambient Intelligence (AmI) technologies and artificial intelligence raises issues related to the ethical and moral obligation of designers in terms of how these technologies might influence and shape warfare in the future. For the military, these technologies may be used to deliberately influence our interactions with each other but they also have the potential for misinterpretation and misunderstanding of commander's intent. Nations and military organizations around the globe have been seeking the benefits of autonomous systems and robotic assets combined with artificial intelligences to change warfare and reduce the loss of human lives during combat. However, the development of such assets would extend the battlespace across all domains, land, sea, undersea, air and space and increase the need for more humans to manage all of these assets. Extending the warfighter's reach via intelligent agent networks and distributed autonomous systems facilitates the extension of the battlespace and the duration of such events. The intent is to provide a more secure global environment with a reduction in required number of military personnel and fewer casualties on a global scale. However, there are significant societal and ethical concerns associated with this 21st century strategy.

How do we protect society against feeling policed in their thoughts and actions? Will these violations of privacy and freedom in combination with advances in AmI intelligent technologies preclude the rules for a Just War?

For society, the combination of these technologies for monitoring, surveillance, and tracking each individual's behaviour and daily life violates our individual sense of privacy and individual freedom. Are we prepared to pay the price to our freedom for national and global security in the 21st Century? Where will we draw the line, if at all, in determining our own course of action? Conversely, will we be content to rely on artificially intelligent systems to dictate our thoughts, beliefs and actions? This is the question for the 21st Century.

"The world is very different now. For man holds in his mortal hands the power to abolish all forms of human poverty and all forms of human life." John Fitzgerald Kennedy

References

Ackerman, E. (2012). *Georgia Tech Robots Learn Deceptive Behaviors from Squirrels*. IEEE Spectrum.

Arkin, R. C. (2012). The Ethics of Robotic Deception. Georgia Institute of Technology College of Computing. http://www.cc.gatech.edu/ai/robot-lab/online publications/deception-final.pdf

Arkin, R. C., & Sukhatme, G. S. (2015). Frontiers of Physically Intelligent Agents: Autonomous Systems for Defense: A Revolution in Military Affairs. *Computing Community Consortium*, Vs.1: June 18, 2015.

Aztiria, A., Augusto, J. C., Basagoiti, R., Izaguirre, A., & Cook, D. J. (2013). Learning Frequent Behaviors of the Users in Intelligent Environments. *Transactions on Systems, Man, and Cybernetics Systems* 43(6).

Barbour, I. (1993). *Ethics in an Age of Technology*. San Francisco: Harper Collins.

Brey, P. (2006). Freedom and Privacy in Ambient Intelligence. *Ethics and Information Technology*, 7(3), 157-166.

Cai, Y., Pavylshak, I., Laws, J., Magargle, R., & Hoburg, J. (2008). Augmented Privacy with Virtual Humans. *Carnegie Mellon University and Ansoft, Inc.*

Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2009). Ambient Intelligence: Technologies, Applications and Opportunities. *Pervasive and Mobile Computing*, pp. 277-298.

Cook, D. J., Augusto, J. C., & Jakkula, V. R. (2007). Ambient Intelligence: Technologies, Applications, and Opportunities. *School of Electrical Engineering and Computer Science, Washington State University and School of Computing and Mathematics, University of Ulster.*

Dilek, S., Cakir, H., & Aydin, M. (2015). Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. *The International Journal of Artificial Intelligence & Applications*, Vol. 6, No. 1, January 2015.

Edgar, J. (2014). Captain Cyborg: The Man Behind the Controversial Turing Test Claims. *The Telegraph*. *Science News*.

Eshel, T. (2016). Russian Military to Test Combat Robots in 2016. Defense Update. http://defenseupdate.com/20151231_russian-combat-robots.html

Foucault, M. (1977). *Power/Knowledge: Selected Interviews and other Writings. 1972- 1977.* New York: Pantheon Books.

Georgia Tech Research Institute. Aware Home Research Initiative. http://www.awarehome.gatech.edu/drupal/

Giordano, J., Kulkarni, A., & Farwell, J. (2014). Deliver us from evil? The Temptation, Realities, and Neuroethico-level Issues of Employing Assessment

Neurotechnologies in Public Safety Initiatives. *Theoretical Medicine and Bioethics*, 35 (1), pp. 73-89.

Guizzo, E., & Ackerman, E. How South Korea's DRC-HUBO Robot Won the DARPA Robotics Challenge. http://spectrum.ieee.org/automaton/robotics/humanoids/how-kaist-drc-hubo-won-darpa-robotics-challenge

Hickman, L. A. (1990). *Technology as a Human Affair*. New York: McGraw-Hill Companies.

Hughes, T. P. (2004). *Human-Built World: How to Think About Technology and Culture*. Chicago: University of Chicago Press.

Jonas, H. (1984). *The Imperative of Responsibility*. *Chicago: University of Chicago Press.*

Kim, D. W., Yang, J. W., & Sim, K. B. (2004). Adaptive Intrusion Detection Algorithm Based on Learning Algorithm. *The 30th Annual Conference of the IEEE Industrial Electronics Society*, Vol. 3, pp. 2229-2233.

Kurzweil, R. (2014). *How to Create a Mind*. Penguin Books, NY.

Kurzweil, R. (2006*). Singularity is Near: When Humans Transcend Biology.* Penguin Books, NY.

Levin, T. Y., Frohne, U., & Weibel, P. (2002). *CTRL [SPACE]: Rhetorics of Surveillance from Bentham to Big Brother.* The MIT Press, First Edition.

Li, X., Feng, L., Zhou, L., & Shi, Y. (2009). Learning in an Ambient Intelligent World: Enabling Technologies and Practices. *IEEE Transactions on Knowledge and Data Engineering*. 21(6).

Rui, L., & Wanbo, L. (2010). Intrusion Response Model based on AIS. *International Forum on Information Technology and Applications (IFITA),* Vol. 1, pp. 86-90.

Masakowski, Y. R. (2015). The Future is Now: The Impact of Ambient Intelligence Technologies on Humans and Warfare. *Proceedings from the 37th Annual Humanities and Technology Conference.* Salve Regina University, Newport, RI.

Masakowski Y. R., & Grasso, R. (2012). Knowledge Elicitation for fuzzy rule-based decision support systems and system interface evaluation and design. *NATO Technical Report: CMRE –FR-2012-009,* NATO Centre for Maritime Research and Experimentation (CMRE), Italy.

Masakowski, Y. R. (2008). Cognition- Centric Systems Design. A Paradigm Shift in System Design. *Proceedings of the COMPIT 08 Conference*. Liege, Belgium

Mitcham, C. (1994). *Thinking through Technology*. Chicago: University of Chicago Press.

Moreno, J. D. (2012). *Mind Wars: Brain Science and the Military in the 21st Century.* New York: Bellevue Literary Press.

Nye, D. E. (2006). *Technology Matters: Questions to Live With*. Cambridge: The MIT Press.

Qiang, H., & Yiqian, T. (2010). A Network Security Evaluate Method Based on AIS. *International Forum on Information Technology and Applications (IFITA)*, Vol. 2, pp. 42-45.

Remagnino, P., & G. L. Foresti. (2005). Ambient intelligence: A new multidisciplinary paradigm. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans* 35 (1): 1-6.

Shim, J. & Arkin, R. C. (2015). The Benefits of Robot Deception in Search and Rescue: Computational approach for deceptive action selection via case-based reasoning. *Presented at the 2015 IEEE International Symposium on Safety, Security, and Rescue Robotics.* Purdue University, West Lafayette, Indiana.

Stanley, M. (1978). *The Technological Conscience: Survival and Dignity in an Age of Expertise*. Chicago: University of Chicago Press.

Postman, N. (1992). *Technopoly: The Surrender of Culture to Technology*. New York: Vintage Books.

Tennenhouse, D. (2000). Proactive Computing. *Communications of the ACM*, 43(5): pp. 43-50.

Treisman, A., & Gormican, S. (1988). Feature Analysis in Early Vision: Evidence from Search Asymmetries, *Psychological Review*, 95, 15-48.

Treisman, A., Vieira, A., & Hayes, A. (1992). Automaticity and Pre-attentive Processing. *American Journal of Psychology*, 5, pp. 341-362.

Verbeek, P. (2009). Ambient Intelligence and Persuasive Technology: The Blurring Boundaries Between Human and Technology. *Nanotechnics*, 3: pp. 231-242.

Wallach, W. (2009). *Moral Machines: Teaching Robots Right from Wrong*. New York: Oxford University Press.

Warren, S., & Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review*, IV (5). Accessed online 15/11/2015.

Winner, L. (1977). *Autonomous Technology: Technics-Out-of-Control as a Theme in Political Thought*. Cambridge: MIT Press.

Wood, C., Towns, S., Knell, N., Pittman, E., & Mullholland, J. (2015). 2015 Digital Cities: Winners Experiment with Forward-Thinking Tech Projects. Digital Communities. http://www.govtech.com/dc/articles/gital-Cities-Survey-2015.html

---

Dr. Yvonne R. Masakowski *is an Associate Professor of Strategic Leadership and Leader Development at the U.S. Naval War College in the College of Operational and Strategic Leadership. Dr. Masakowski has a distinguished career in Human Factors and Systems Design spanning over twenty years. Previously, Dr. Masakowski was the Lead for the Human Performance & Technology Group in the Advanced Concepts Division at The Naval Undersea Warfare Center in Newport, RI. She is currently serving as the U.S. Chair for NATO's Panel on "Leader Development for NATO Multinational Military Operations." She earned her Ph.D. from City University of New York.*

Jason Spencer Smythe *is a crime analyst at Danville, VA Police Department. He conducted Ethics and Emerging Military Technology research at the U.S. Naval War College. Jason earned his Master of Forensic Psychology from Roger Williams University and has a specialty in Counterterrorism.*

Dr. Thomas E. Creely *is Associate Professor of Ethics, College of Operational and Strategic Leadership, at the United States Naval War College. Dr. Creely is the Lead for the Ethics and Emerging Military Technology Graduate Certificate, as well as the Effective Leadership Lead for Brown University's Executive Master in Cybersecurity. He has taught at universities in Georgia and South Carolina and consulted with corporate executives. Dr. Creely serves as Global Business Conduct Council Member on The Conference Board, Business Ethics Co-chair with Association for Practical and Professional Ethics, and Treasurer of Robert S. Hartmann Institute Board. He earned his Ph.D. from Salve Regina University.*