2007

Users' Adoption of Emergent Technologies: Towards an Acceptable Model for Safer Cyber-Assisted Olfactory Information Exchanges in Standard, Micro, and Nano Systems

Berg P. Hyacinthe

THE FLORIDA STATE UNIVERSITY

COLLEGE OF INFORMATION

USERS' ADOPTION OF EMERGENT TECHNOLOGIES: TOWARDS AN ACCEPTABLE MODEL FOR SAFER CYBER-ASSISTED OLFACTORY INFORMATION EXCHANGES IN STANDARD, MICRO, AND NANO SYSTEMS

By

BERG P. HYACINTHE

A Dissertation submitted to the
College of Information
in partial fulfillment of the
requirements for the degree of
Doctor of Philosophy

Degree Awarded:
Summer Semester, 2007

The members of the Committee approve the Dissertation of Berg P. Hyacinthe defended on June 21, 2007.

John N. Gathegi
Professor Directing Dissertation

Xiuwen Liu
Outside Committee Member

Darrell Burke
Committee Member

Mia L. Lustria
Committee Member

Approved:

Larry Dennis, Dean of the College of Information

The Office of Graduate Studies has verified and approved the above named committee members.

This manuscript is particularly dedicated to my beloved daughter

Cynthia Shana Elle

I also dedicate this document to a senior Test Systems Engineer at Motorola

Sophia Shona Hunt

Moreover, I must acknowledge the continuous sacrifices of my parents

Rev. Gédéon Hyacinthe (my dear father)

Elina Rose Plancher Hyacinthe (my mother)

Particularly and gratefully to the great Hunt family

John Sr., Elma, Venton, Anestasia, John Jr., Curtis, and Diana

ACKNOWLEDGEMENTS

I thank the Heavenly Father for his blessings and strength. I thank Dr. John Gathegi for his prescient identification of this endeavor as an ambitious and very challenging one and for his decision to support the project from start to finish. A special thank you goes to my dear and faithful committee members: Dr. Darrell Burke, Dr. Mia L. Lustria, and Dr. Xiuwen Liu. A special thank you goes to Dr. Ned Stuckey-French for assisting me during the final stage of this report.

I want to thank those who supported my idea to enter this doctoral program (James Mudd and Leo Ochs –Manager and Deputy Manager of Collier County Government, Florida). I also thank Skip Camp (Collier County Government) for opportunities to work on several post-*911* security projects (including early implementation of web-based video surveillance technologies ubiquitously installed around the world today). And thanks to retired FBI agent Harold Copus and Officer Francine Ware.

I will forever be grateful to my best friend Brunel Excéus, to my mentors Aramentha Raymond Excéus (Toune), Dr. Jacqueline Duplésis-Duperval (Caco), and to my teachers Alphonse St. Louis, Dr. Elie Plancher (MD), belated Michael Plancher, Prospère St. Imé, Sandy Walter Turnbull, and to the entire Hyacinthe and Plancher families (Dave on both sides). To Lucie, Thérèse, Tifa, and Ms. Marion Davis, Merci!

Finally, I wish to thank Zia Hayat of BAE Systems, UK, Dr. Boukhtouta of Defence Canada, Monsieur Goretta of France Defense Department (DGA), Dr. Popp of U.S. DARPA (Defense Research Program Agency) for their initial feedback on the autonomous biochemical defense concept. The merit belongs to many people within the international intelligence community who will not be identified by name because of the nature of what they do. THANK YOU!

TABLE OF CONTENTS

LIST OF TABLES vii
LIST OF FIGURES viii
LEXICON AND ABBREVIATIONS LIST ix
ABSTRACT xiii
CHAPTER I: INTRODUCTION 1
BACKGROUND 1
PURPOSE OF THE STUDY 8
PROBLEM STATEMENT 8
PRIMARY RESEARCH QUESTION 10
SIGNIFICANCE OF THE STUDY 11
CONCEPTUAL FRAMEWORK 12
RESEARCH OBJECTIVES 13
CHAPTER SUMMARY 14
CHAPTER II: LITERATURE REVIEW 15
THEORETICAL PARADIGMS 16
KEY CONCEPTS 22
PRAGMATIC APPROACH TO LESSONS LEARNED 27
HYPOTHESES 28
CHAPTER SUMMARY 29
CHAPTER III: RESEARCH METHODOLOGY 31
CONCEPTUAL DESIGN 31
RATIONALE 32
USE OF BLOCK-DIAGRAMS JUSTIFIED 37
EMPLOYMENT OF SCENARIO PLANNING JUSTIFIED 38
STANDARD AND LAB-ON-CHIPS EMBODIMENTS ILLUSTRATED 40
DESIGN OF THE STUDY 46
METHODOLOGY JUSTIFIED 49
ESTABLISHMENT OF CONSTRUCTS 51
RESEARCH PROTOCOLS EXPLAINED: METHODS AND PROCEDURES 55
CHAPTER SUMMARY 60

CHAPTER IV: DATA ANALYSIS AND INTERPRETATION OF RESULTS 62
COMPARATIVE CONTENT ANALYSIS 62
INTERNET AS TERRORIST TRANSPORT VEHICLE OF WMD 65
DISCUSSION OF SURVEY RESULTS AND VALIDATION OF HYPOTHESES 67
HYPOTHESES AND TEST RESULTS 69
CHAPTER SUMMARY 78
CHAPTER V: PRESCRIPTIONS AND CONCLUSIONS 80
WARNINGS AND PRESCRIPTIONS 81
FURTHER RESEARCH AND PRESCRIPTIONS 83
CONCLUSIONS 83
APPENDIX A: FSU HUMAN SUBJECTS APPROVAL LETTER 87
APPENDIX B: FAMU HUMAN SUBJECTS APPROVAL LETTER 88
APPENDIX C: INFORMED CONSENT FORMS AND SURVEY INSTRUMENT 89
APPENDIX D: ABSTRACTS OF REVIEWED PATENTS 94
APPENDIX E: DECLASSIFIED MILITARY ABSTRACTS 100
APPENDIX F: YESTERDAY'S DIRTY UNMANNED AIR VEHICLES (UAVS) 109
APPENDIX G: TODAY'S NANO AIR VEHICLES (NAVS) 111
APPENDIX H: MISCELLANEOUS SPSS OUTPUT DATA 113
APPENDIX I: POWERPOINT SLIDES OF MULTIMEDIA COMPONENTS 121
APPENDIX J: RESEARCHER'S PRAGMATIC APPROACH TO LESSONS LEARNED 130
APPENDIX K: WARNINGS AND MAJOR ATTACKS 136
REFERENCES 137
BIOGRAPHICAL SKETCH 153

LIST OF TABLES

TABLE 1: MICHAEL BUCKLAND'S FOUR ASPECTS OF INFORMATION 5
TABLE 2: THREE-FACTOR ANOVA RESULTS (SPSS 15.0) 58
TABLE 3: SNAPSHOT OF CONTENT ANALYSIS OF PATENTS AND REPORTS 64
TABLE 4: SEVEN FINDINGS FROM THE COMPARATIVE DATA ANALYSIS 67
TABLE 5: DEMOGRAPHIC INFORMATION (GENDER) 68
TABLE 6: CLASSIFICATION BY ENGINEERING MAJORS 70
TABLE 7: DESCRIPTIVE STATISTICS FOR HYPOTHESIS #1(SPSS) 71
TABLE 8: CORRELATIONS BETWEEN CONSTRUCTS (SPSS) 72
TABLE 9: T-TEST RESULTS (H_1) 73
TABLE 10: CORRELATION COMPUTED USING SPSS (H_2) 74
TABLE 11: ANOVA BETWEEN CREDIBILITY AND USEFULNESS (SPSS) 75
TABLE 12: AGREEMENT RATIOS FOR HYPOTHESIS #2 (SPSS) 75
TABLE 13: MEAN SCORES FOR USEFULNESS, EASE-OF-USE, AND CREDIBILITY 77
TABLE 14: SUMMARY OF TEST RESULTS FOR THE FIVE HYPOTHESES 78

LIST OF FIGURES

FIGURE 1: CONCEPTUAL FRAMEWORK 13
FIGURE 2: CONVERGENCE OF PATENT SEARCH AND MILITARY REPORTS 15
FIGURE 3: LIGHT-SCATTERING DETECTION TECHNIQUE 25
FIGURE 4: PRIMARY HYPOTHESIS ILLUSTRATED 29
FIGURE 5: DAVIS' (1989) TECHNOLOGY ADOPTION MODEL 34
FIGURE 6: INFLUENTIAL RELATIONSHIPS BETWEEN CONSTRUCTS 36
FIGURE 7: SCHEMATICS FOR THE STANDARD EMBODIMENT OF THE ABCD 41
FIGURE 8: (A, B, & C) MODEL FOR SAFER CYBER-ASSISTED OLFACTION 42
FIGURE 9: APPLICATIONS IN AVIATION, MASS TRANSIT, AND DWELLINGS 44
FIGURE 10: 1-2-3 OF THE ABCD 46
FIGURE 11: ORIGINAL CONCEPTION OF THE CONSTRUCTS 55
FIGURE 12: HISTOGRAMS AND SAMPLE MEAN SCORES 72
FIGURE 13: GENERAL EQUATION FOR CORRELATION COEFFICIENT 73
FIGURE 14: OBSERVED ACCEPTABILITY OF THE MSCAO 79
FIGURE 15: AGREEMENT/DISAGREEMENT TO THE PROPOSED MSCAO 85

LEXICON AND ABBREVIATIONS LIST

This lexicon is a reference guide to the reader. Although the researcher has been very prudent about the use of unnecessary jargon, unfamiliar and new constructs naturally necessitate contextual and lexical definitions. Accordingly, due to the nature, complexity, and novelty of the chosen topic, it was essential to delineate definitions for this dissertation. Firstly, readers of this manuscript may not be able to understand what has been written unless they clearly understand the taxonomy of knowledge being established and the lexicon being used. Secondly, participants in this study could have provided inaccurate information if they misinterpreted questions based on false premises (i.e., if the terms and concepts are not clearly defined and presented). For the foregoing reasons, the researcher prepared a glossary accompanied with brief definitions of some of the key expressions and acronyms. This alphabetically ordered lexicon was built according to guidelines established in (Hutchins and Hazlehurst, 1995) to provide a platform of shared symbols between the researcher and his audience:

Aroma-embedded Information Systems: Refer to systems that facilitate olfactory information exchanges for technologies such as scented emails and fragrance-embedded websites.

Biosensors/E-noses: Electronic noses (also known as biosensors) are instruments which mimic the sense of smell. They consist of olfactory sensors and a suitable signal-processing unit; they are able to detect and distinguish odors precisely and at low cost.

Cyber-assisted Olfaction: Refers to the stimulation of human senses by computer-emitted chemical particles or fragrances.

Cybernetics: Inline with Wiener's (1948) introduction, Cybernetics is defined as the replication or imitation of biological control systems with the use of technology.

Cyber-WMD Nexus: An expression first coined by the researcher in 2004 to refer to the potential misuse of the Internet as a transport vehicle of WMD: a lethal symbiosis between computer networks and weapons of mass destruction. The researcher calls it "a new form of cyber warfare" (Hyacinthe, 2006c).

Enskog Theory: This theory reveals a framework to study how chemical particles bind through different mechanisms, in particular through thermal energy. Principles related to this theory have been extended to other sources of energy.

Information: Information, as a concept, is defined by the researcher as a *meaningful differential* that emerges from one or multiple interactions.

Information Science: Information science is accepted as a discipline that is concerned with the study of information to include creation, storage, exchange, and retrieval. To avoid any confusion with information system, information science will not be referred as IS in this dissertation.

Information Technology (IT): Covers all mechanisms, processes, and materials involved in the creation, storage, and distribution of all types of information (e.g., vibratory and olfactory information). IT is manifested in computer hardware, software, and peripherals. IT is at the core of digital information systems (IS).

Information Warfare (IW): IW is viewed as a psycho-socio-economical warfare enterprise that uses evolving information technologies and theories as visible and invisible weapons to conquer the mind through anticipative identification and usage of information signatures and opportunities, in order to overcome conventional warfare constraints and ineffectiveness.

Innovation Diffusion: Innovation diffusion, according to Rogers (1995), encompasses all technology diffusions, not just information technology. Nonetheless, innovation diffusion is used in this dissertation in the context of a model for safer cyber olfaction technologies.

Lab-on-Chip (LoC): Refers to the realization of a functional laboratory at a very low (micro- or nano-) scale on computer chips. LoC technologies are not limited to fluid circulation. Microfluidics and Micro Total Analysis System (μTAS) are LoC applications.

Latent Variables: Refer to variables not directly observed but are rather inferred from other variables that are observed and directly measured. In this study, adoptability is considered as the latent variable.

Microfluidics: Refers to technologies or a series of mechanisms that process fluids at a very low scale (micro and nano levels). These technologies are prevalent in μTAS.

Micro Total Analysis System (μTAS): Although this term is often used interchangeably with LoC and microfluidics, μTAS, in this study, refers specifically to micro systems that sample, detect, test, and process biochemical activities under the sub-millimeter regime (e.g., micro- and nano- scales).

***MSCAO*:** is short for Model for Safer Cyber-Assisted Olfaction. It is to be pronounced as "Mess-Cow" to refer a Judeo-Hindu derrivative.

Observable Variables: Refer to the constructs from which information is being observed. They are the variables that have been scaled in order to generate scores for usefulness, ease-of-use, and credibility.

Olfactory Information Warfare: Refers to the use of aroma-embedded information systems to conduct war. It is a form of cyber warfare.

Perceived Acceptability: Acceptability measures the degree of tolerance of the system. In this context, it is assumed that the students are likely to accept a tolerable technology and invest the required resources in order to benefit from its usefulness. Information technology adoption can be defined as the decision to accept, or invest in a technology (Davis, 1989, emphasis added).

Perceived Ease-of-Use: Refers to the degree of difficulty of the system to assist a user with the completion of a task. Other terms associated with this construct include effortless, flexibility, and easiness.

Perceived Feasibility: The degree of feasibility of a model indicates how likely the system (represented) is to be accepted and adopted. It is also a predictor of how likely the resulting product is to move from model to fabrication.

Perceived Usefulness: Refers to the purposefulness of the system as it relates to performing an important task such as solving a problem, satisfying a need, or addressing a threat. Usefulness, in this context, is an epithet of efficacy, helpfulness, and worthiness.

Prescriptive Research: A prescriptive research is conducted with the intent to offer a remedy to a situation and/or make constructive recommendations on how to address an issue that has been thoroughly investigated.

Silver Bullet: Silver bullet implies the use of a single decontaminant that is effective against all dangerous chemicals (i.e., one synergistic solution to multiple problems).

Social Informatics: Based on Kling's (2000) definition, social informatics accounts for cultural and social interactions involved in information technology diffusion and adoption. As the present researcher puts it, "social informatics involves a majestic interplay between social evolution and technological innovation."

'**Standard**' **Systems:** Account for systems that use common measurements or regular scales (e.g., regime above micro- and nano- scales).

Scenario Planning: Refers to a strategic planning technique used to make flexible long-term plans. It is used in this study in the context of technology forecast and diffusion.

Techno-terrorism: Refers to the use of technology to spread terror through physical disruption, according to Littleton's (2005) definition.

Terrorism: Terrorism here indicates the use of terror to achieve an objective; it is not to be used loosely or associated with any political agenda or discriminatory practices.

WMD: This is an acronym for *weapons of mass destruction*. Biological and chemical warfare agents are considered as such weapons.

ABSTRACT

The potential of terrorists and other enemies to use the Internet and/or other digital information technologies as transport vehicles of weapons of mass destruction (WMD) is becoming more evident. This threat may involve cyber-assisted biochemical transactions, which can be performed through olfactory information exchanges, to attack civilian and military targets anytime. In response, this research is the product of a four-year investigation wherein the researcher went through a rich archive of declassified U.S. military reports (covering biochemical warfare and techno-terrorism)and a selective list of patent applications revealing several concepts related to users' adoption of emergent cyber-assisted olfaction and *aroma-embedded information* systems. And after a rigorous analysis of the findings, the researcher hypothesized that careless adoption of unsafe technologies could accelerate a cyber-WMD-nexus.

Thus, the study conducted in support of this research sought to examine and explain the adoption of emergent cyber-assisted olfactory information technologies. Cyber-assisted olfaction is an emergent technology that involves the replication of the human sense of smell by computer systems. It can be manifested in the stimulation of human olfactory receptors by computer-emitted biochemical or aromatic particles. Certain olfaction-based biosensors, known as electronic noses, mimic the sense of smell to detect chemical plumes (aroma or warfare agents) in a variety of settings. Notably, the literature revealed an innovative dimension of multimodal, affective human-computer interactions involving scented emails, aroma therapy, and olfaction-based marketing. Unfortunately, the lack of security and safety persists at a potentially catastrophic cost, which is at the root of the researcher's stated research problem below.

Largely supported by Everett Rogers' innovation diffusion theory (IDT) and Fred Davis' technology acceptation model (TAM), the researcher went beyond the "smell-o-vision" aphorism to offer a fertile ground for a new, comprehensive, and flexible framework to understand various aspects of cyber-assisted olfactory information systems, which may be usefully applied to a wide range of auxiliary information systems (i.e., standard, micro, and nano devices). In relation to national security and defense, the proposed Model for Safer Cyber-Assisted Olfaction (*MSCAO)* can be applied in subway systems, aircrafts, cruise ships, and various mixing/distribution systems (i.e., water systems and chemical plants) to automatically

detect and neutralize a biological or chemical threat. Many military applications are also anticipated for emerging urban warfare and emergency rescue operations using devices such as miniature robots and nano air vehicles (NAVs).

Consistent with the aim of this investigation, the researcher used a mixed-methods approach that combined (1) the content analysis of a series of declassified military reports on airborne warfare agents with that of (2) a patent search on aroma-embedded information systems to examine, with the help of a carefully designed survey instrument, the perceptions of potential adopters of the proposed *MSCAO*. Further, in order to collect data and obtain statistical evidence linked to the selected variables (perceived *credibility, ease-of-use,* and *usefulness*), the researcher surveyed a diverse group of students from a major Engineering School in southeastern United States, which offers degree programs in Mechanical, Electrical, Chemical and Biomedical Engineering. Based on the analysis performed, credibility, ease-of-use, and usefulness were found to be significant enough to be considered as positively influencing the acceptability of the *MSCAO*. In essence, the respondents expressed a significantly high level of need for harm-reduction and cyber security measures against potential threats and considered the MSCAO as meeting their need.

Perceived usefulness (67%) was identified as the principal determinant of the respondents' intention to adopt the proposed model. Though less substantial than perceived usefulness, perceived ease-of-use (56%) appeared to have a greater influence on the *MSCAO* than perceived credibility (54%).

In sum, extrapolating from the findings reported herein, the researcher concluded that potential users are more likely to accept an emergent technology that is useful, easy-to-use, and that offers credible harm-reduction measures.

CHAPTER I: INTRODUCTION

BACKGROUND, PURPOSE, PROBLEM STATEMENT, RESEARCH QUESTIONS, SIGNIFICANCE, CONCEPTUAL FRAMEWORK, AND RESEARCH OBJECTIVES

BACKGROUND

This study aimed to examine and explain the adoption of emergent information technologies. Cyber-assisted olfaction is an emergent technology that involves the replication of the sense of smell by computer systems. In particular, it can be manifested in the stimulation of human olfactory receptors by computer-emitted biochemical or aromatic particles. Certain olfaction-based biosensors, known as electronic noses, mimic the sense of smell to detect chemical plumes (aroma or warfare agents) in a variety of settings. In the fields of Photonics and Biomedical Engineering, the academic literature abundantly covers advances in biosensor technologies (Collings and Caruso, 1997; Dariva *et al.,* 1999; Fair *et al.,* 2004; Frye-Mason *et al.,* 2000; Preston and Mc Fadden, 2001; Srinivasan *et al.,* 2003; Srinivasan *et al.,* 2004). Also, Bioinformatics has emerged, in a relatively short period of time, as a quintessential link between established information theories, molecular biology, computer engineering, medicine/tele-medicine, and defense and security -to facilitate the design of DNA-based detection systems, micro-electromechanical systems (MEMS), and micro total analysis systems (μTAS). Unfortunately, in spite of the obvious risks and documented warnings from defense and security experts around the world regarding the lack of security and safety, the problem persists. In response to this need, the researcher focused on two major dimensions of cyber-assisted olfaction: (1) MEMS-based autonomous biochemical detection/neutralization systems covering security protocols and harm-reduction measures for a safer cyber-assisted olfactory information exchange environment and (2) aroma-embedded information systems primarily involving technologies such as scented emails, fragrance-enabled websites, and aroma-enabled avatars for entertainment and e-commerce applications through the Internet.

The rise of the Internet is often portrayed as a major explosion. This “explosion” metaphor is also deeply rooted in information science literature. As such, much earlier, Bush (1945) warned of an “information explosion” and proposed a solution, using emergent information technologies to address the related challenges. In addition, Claude Shannon (1949) implicitly used explosion of *digital noise* to secure information channels as described in his law of perfect information secrecy.

Shannon's model for perfect secrecy was designed to allow a pair of secure computers to communicate over an insecure (very noisy) link. Contrary to previous attempts to portray the Internet as an isolated electronic explosion that took place in the abstract world of cyberspace, recent research findings have shown how the Internet is embedded in everyday life (McFarland and Hamilton, 2006; Ahlqvist, 2005; Fogg, 2003; Sperberg-McQueen *et al.*, 2000; Murray, 1997). In addition to the literature related to the spread of Internet, the researcher drew from Rogers' (1995) innovation diffusion theory and Davis' (1989) technology acceptance model in order to support his examination of users' adoption of emergent information technologies. In many instances (Venkatesh and Davis, 2000; Gefen and Straub, 1997; Karahanna *et al.,* 1998; Wang and Benbasat, 2005; Al-Gahtani, 2001), an additional perception-based construct was added to the latter theories (as done in the present study) to address research particularities.

Emergent Technologies as Terrorist Weapons

The potential of terrorists and other enemies to use the Internet and other emergent digital information technologies as transport vehicles of WMD is becoming more evident. Hence, from the continuous proliferation and mutation of biochemical warfare agents (such as the 1930's organophosphates) to dual-use chemical facilities during the 20th century onward, a more threatening mutation paradigm has clearly emerged: morphing common substances and apparati into WMD. The adoption of this paradigm by sectarian groups (a seemingly unanticipated challenge) has drawn a very blurry line between conventional and unconventional warfare practices and compelled defense and security officials onto unprecedented intelligence reforms. For instance, in 2004, the U.S. Congress passed the Intelligence Reform and Terrorism Prevention Act, mandating the Director for National Intelligence (DNI) to oversee and coordinate all intelligence collection in order to advise Congress and the White House. Due to the latter reorganization, the director of the CIA no longer reports directly to the president (DNI, 2007). In fact, a decade earlier, Harry Stonecipher, President and CEO of Mc Donnell Douglas warned that "*increasingly sophisticated weapon technology would eventually fall into the hands of disaffected nations, groups or even individuals and that as a result the challenges facing political and military leaders would become harder rather than easier*" (Adams, 1998, p. 298).

Emergent technologies encompass but are not limited to highly selective drugs, sensors, new explosive materials, newly discovered biochemical threats

(toxins, bacteria, viruses), integrated information and communication systems, semi-autonomous robots, miniature robots, photonics, nanotechnologies, intelligent materials, revolutionary algorithms, and notably biologically-inspired, multimodal sensing systems.

Today, several background phenomena and events have embodied the researcher's prescient mutation paradigm including widely reported official accounts of (1) aircrafts intelligently morphed into missiles to destroy human lives and dismantle several critical infrastructures in the United States, (2) cars transformed into rockets-on-wheels, (3) cell phones modified into remote detonators, (4) smoke detectors explored as sources of radioactive materials, and (5) common containers (normally used to store medicines and cosmetic products) exploited as carriers of liquid explosives. In the latter instance, British intelligence officials thwarted an alleged terrorist plot, possibly just days away, to blow up U.S.-bound jetliners over the Atlantic in an attempt to kill thousands with liquid explosives concealed in water bottles and other common containers.

Terrorism is an overused, seemingly abused, and certainly very controversial term. It is not to be limited to a particular group or specific religious background. Unfortunately, regardless of the definition considered, terrorism involves fear and violence. In fact, the following is true regarding terrorism: *it will mutate with emergent* technologies. In order to deal with the atypical cyber-conditioned and *techno-terrorists* of the future, the on-going fusion of computers and digital information technologies with weapon systems will need to be studied and understood according to a multidimensional perspective (Hyacinthe *et al.*, 2007), an exploration that goes beyond the scope of this dissertation.

Versatility of Information Professionals

Information professionals are inherently familiar with the basic information exchange principles that govern most *systems*. Some have mastered these principles according to various paradigms and use the acquired knowledge to serve as devoted librarians, policy makers, health professionals, law enforcement and intelligence analysts, defense and security experts, and so forth. For example, librarians quietly served as double (information) agents during the Cold War against the spread of the former Soviet regime; but they came close to be discounted as national security threats when they rightfully challenged certain provisions of the controversial U.S.

Patriot Act[1] (part of a controversial legislation passionately promoted and defended in its entirety by the administration of U.S. President George Walker Bush).

Historically, regardless of their particular orientation, wary and highly trained information scholars possess the rare ability (and benefit from their natural professional advantage) to conduct cross-, multi-, and inter-disciplinary research (Bush, 1945; Shannon, 1949; Shannon and Weaver, 1949; Hyacinthe, 2006a; Gathegi, 2005; Hyacinthe, 2006c; Kanzaki *et al.*, 2005; Kuhlthau, 1991). As the literature review suggests, the Internet adds on to, rather than diminishes other forms of communication. However, as *new types* of information emerge, ubiquitous and open networks introduce new information security risks due simply to a more complex system which has a greater threat space. Consequently, in order to protect such networks, pro-active measures must be taken, enabling computer security risk owners to make more informed decisions on the trade-off between providing or preventing additional functionality (Hyacinthe *et al.*, 2007). Before discussing these *new types* of information any further, the *problem of information*, as Raber (2003) would put it, deserves some thoughtful considerations.

Multidimensional Nature of Information

Three concepts emerged when Dr. Samuel Johnson discussed the meanings of information in his 1755 English Dictionary: (a) intelligence given/instruction, (b) charge or accusation exhibited, and (c) the act of informing or actuation (Capurro and Hjørland, 2003). Taking a different approach, when Saracevic (1999) presented his personal analysis of information science as a field of scientific inquiry and professional practice, he offered his 'scientific' definition of *information* as "*We Don't Know*" (p. 1054). In essence, he meant that lexical definitions only provide restrictions on basic phenomena such as information, life, energy, and so on.

Ironically, although they were "working definitions," a number of meanings surfaced in Saracevic's article (p. 1054):

(1) *Information* is considered in terms of signals or messages for decisions involving little or no cognitive processing, or such processing that can be expressed in algorithms and probabilities (narrow sense).

[1] Although a new legislation might have been needed to address certain threats against the United States and its allies, history is likely to show that several *unnecessary* provisions ended up hurting the United States and its citizens profoundly. Yet, due to certain practices authorized by the act itself, the number of victims might never be known.

(2) *Information* is treated as directly involving cognitive processing and understanding (broader sense).

(3) *Information* is dealt with in a context. That is, information involves not only messages (narrow sense) that are cognitively processed (broader sense), but also a context such as a task or problem at hand (broadest sense).

In addition, when Buckland (1991) was faced with a variety of meanings (Machlup, 1983; Braman, 1989; Schrader, 1984), he took a pragmatic approach. He defined information in terms of its principal uses or *meanings*: information-as-process, information-as-knowledge, and information-as-thing (p. 351). In Table 1, the parallelism established between tangible and intangible information also relates to the four aspects of information (not to be confused with three meanings) of Buckland (1991, p.352).

Thus, the researcher's discussion of "olfactory information processing" is held within the context of Buckland's *process* (third row of Table 1), which encompasses data processing (tangible) and becoming informed (intangible).

Table 1: Michael Buckland's four aspects of information (p.352)

	Intangible	***Tangible***
Entity	Information-as-Knowledge Knowledge	Information-as-Thing Data, Document
Process	Information-as-Process Becoming Informed	Information Processing Data Processing

Notably, Shannon and Weaver (1949) established a measure of information in terms of purely physical quantities through what appears to be a deliberate attempt to eliminate the 'psychological factors' involved in this information concept.

It would be an oversight to discuss the evolution of information science as a field without a special acknowledgment of Vannevar Bush (1945). Bush was a respected MIT scientist and the head of the scientific effort during World War II. He addressed the problem of '*information explosion*' well before the so-called *cyber revolution*. Accordingly, Saracevic (1999, p.1053) characterized Bush's foresight as a prescient anticipation of information science and artificial intelligence. It is worth noting that since the late 1980's, scientists have turned attention to neural nets in

order to model cortical functions on computers (Patels, 1988). Even Thomas Aquinas' theory of knowledge (intellectus/sensus) appeared to be supportive of this relationship between the external world and the internal world, between biological systems and external stimuli.[3] Essentially, Aquinas posits that what takes place inside the mind has a lot to do with what our senses communicate to it (the mind). His disciples later insisted on harmony or balance between the body and the mind. Nonetheless, the *problem of information* remains very complex.

Citing Buckland's *Information-as-thing,* Raber (2003) exposed the problem of information in these terms:

"If we take the word [information] to represent any object or phenomenon that might be informative, "then everything is, or might well be, information" (p. 1).

Although Raber presented his readers with a problem, he did not offer any pragmatic solutions. It is fair to note that Raber's focus was not on definitions or answers *per se* but on exposition and discourse: a legitimate dialectic strategy to elicit knowledge. Raber opened a wider discourse around cognitive and physical paradigms.

In summary, the researcher shares Buckland's assertion of information as any object or phenomenon that might be informative. In the present context, for example, an informative Internet session may involve the online purchase of a particular product (such as a perfume) wherein information exchange occurs between the aroma-embedded Web space and the buyer –from the epithelium, through the olfactory bulbs, into the brain.

Sensory and Olfactory Information Exchange

To better understand how information is sought, accessed, and used, one must investigate how users process information from the different senses, not only through the traditional auditory and visual channels. As such, a well-trained information scientist may focus not only on how information from each sensory modality is decoded but also on how this information fluctuates with the sensory processing taking place within other sensory channels such as vibration, degustation, and olfaction.

---

[3] http://radicalacademy.com/aquinas2.htm#knowledge [Thomas Aquinas]. Last download, June 25, 2007.

For instance, neurotransmitters, the key information molecules of the brain, mediate the actions of chemicals and drugs in the central nervous system. As the literature suggests, these molecules account for diverse chemical classes, including the biogenic amines, amino acids, peptides, and gases (de Gelder and Bertelson, 2003; Cain and Murphy, 1980; Phillips and Silverstein, 2003). Thus, the inhalation of any chemical will activate (at least) one of these “information processors/receptors.”

It is equally important to note that olfactory information exchange involves principles of exchange that have been adopted in information seeking behavior, information need, information access and robotics. For example, olfactory information exchanges follow the standard sender-channel-receiver path, in which case the sender generates a code that travels through a network channel (such as the Internet) to activate a particular fragrance container at the receiver’s end.

Computers process olfactory information through electronic noses (also known as e-noses or biosensors). Essentially, "e-noses" are very useful for a remarkable variety of applications in the food and pharmaceutical industry, in environmental control or clinical diagnostics and detection of dangerous chemicals (Srinivasan *et al.*, 2003; Baeumner *et al.*, 2001; Eigen *et al.*, 1994, Ishida *et al.*, 1996).

Cyber-Assisted Olfaction

One of the latest additions to the Internet is what is here referred to, and identified as, cyber-assisted olfaction. In order to avoid any confusion, cyber-assisted olfaction is defined here as the stimulation of human senses by computer-emitted chemical particles or fragrances. This claim relates only to the use of the term, not the concept. In fact, Heilig’s (1962) was one of the earliest serious attempts to build an aroma-embedded computer information system. Subsequent attempts include Barfield and Danas (1995) who commented on the use of olfactory displays for virtual environments and Wisneski (1999) who discussed ambient environments. Nonetheless, what is significant about this study is its emphasis on cyber-assisted olfactory information security and autonomous biochemical decontamination processes in various settings.

For example, cyber-assisted olfaction may involve (1) olfactory information exchanges (i.e., sharing scented email) between two computer users, (2) the dispersion of an airborne biochemical warfare agent by a digital apparatus towards a human target, or (3) a computer-controlled release of a neutralizing substance to

mitigate (Russell *et al.*, 2003) the harmful effects of an offending chemical or biological agent. It is important to note that preliminary findings already pointed to the Internet as an indirect (e.g., sophisticated knowledge sharing) transport vehicle of WMD (Torrens, 1999).

Summing up, in response to this potential cyber-WMD nexus, which is at the core of the research problem, the researcher built a comprehensive theoretical framework for safer cyber-assisted olfactory information exchanges.

PURPOSE OF THE STUDY

Computer users continue to exchange information in nanoseconds via an array of digital devices with the potential to be morphed by terrorist groups and/or other enemies into ubiquitous weapons. This study sought to determine potential users' perceptions regarding the adoption of a security model for safer cyber-assisted olfaction technologies according to Davis' (1989) TAM. In this regard, the researcher explored harm-reduction measures that might be built-into cyber-assisted olfaction systems to make them more acceptable to potential users. Furthermore, systems that emerge from the proposed model for safer cyber-assisted olfaction (MSCAO[4]) system may be applied in aviation and mass transit security to initiate mass decontamination by dispersing an aerosolized decontaminant or to protect the public water supply against a potential bio-terrorist attack via an olfaction-based detection and suppression technique.

PROBLEM STATEMENT

The proliferation of WMD and the use of such elements pose an imminent threat with disastrous consequences to the national security of any nation. In particular, the use of biochemical warfare agents against civilians and unprotected troops in international conflicts or by terrorists[5] against civilians is considered as a real threat. In spite of the current surge to come up with effective countermeasures against such threats (Singh and Singh, 2003; Radnedge *et al.*, 2001; Ewing *et al.*, 2001; Jankowski *et al.*, 1992; Sutton *et al.*, 2005), existing solutions remain passive in nature while the threat continues to mutate with each technological innovation (Hyacinthe, 2006b). This problem is accentuated by the emergence of unsafe aroma-

[4] MSCAO is to be pronounced "Mess-Cow" (see Lexicon and Abbreviations List).
[5] Terrorism here indicates the use of terror to achieve a means; it is not to be associated with any political agenda or discriminatory practices.

embedded and other types of olfactory information systems. Evidently, new waves of terror attacks have changed the rules of information sharing and consequently caused wary information scientists to refocus their investigative lenses on "new types" of information use, processing, transfer, and security. Hence, to meet the information needs of the future, information science researchers may have to embark in innovative research related to intelligence analysis (Clark, 2003; Garst and Gross, 2005), information warfare (Libicki, 1995), and olfactory information processing (Kanzaki *et al.*, 2005). In effect, the latter element is inline with the common goal of information scientists, computer experts, information practitioners, government agencies, and the corporate world to avail safe information[6]. Unfortunately, the threats to cyber-assisted olfaction systems are real, and there is a lot more to be learned about users' adoption of new and emerging technologies before effective solutions may be introduced.

Particularly, little information is available on engineering college students' perceptions regarding the adoption of cyber-assisted olfaction technologies. Less is also known about the decision-making process potential adopters of emergent technologies use to determine whether aroma-embedded information systems, for example, would be safe enough under the specific conditions presented to them. How can these issues be resolved?

Diffusion of innovation, a theory applied most directly to communication studies (Rogers, 1995; Basu and Fabre, 1992; Carley, 1996), is also the acknowledged starting place for studies attempting to describe implementation and use of new technologies. According to Rogers, adoption behavior is the relationship between the time at which individuals choose to adopt a technological innovation and the time at which other members of their social setting do so: an intersecting principle between Social Informatics and Social Network Analysis. Very often, innovations go through a process of re-invention in which the innovation is changed or modified by a user in the process of its adoption and implementation. Mainly based on the foregoing analysis, the researcher hypothesized that the respondents' responses are likely to shed new light on counter-measures and security protocols clearly needed to render cyber-assisted olfaction technologies safer to intended users.

[6] Selective and/or encrypted (e.g., customized passwords, confidential documents, and military secrets).

Finding the right method to evaluate a technology that is not fully tested is a challenge that necessitates a careful consideration of authoritative theories and existing models. This research benefited enormously from the conjugation of Rogers' (1995) innovation diffusion theory with Davis' (1989) technology acceptance model to address the above concerns.

A methodological scheme was established in order to identify and clarify the research problem, which is summarized in the following statement: since preliminary content analyses revealed that aroma-embedded information systems were emerging rapidly without any standard security protocols, a comprehensive model for safer cyber-assisted olfactory information exchanges was greatly needed. The most logical step was to focus on how and why users would adopt this type of technology.

PRIMARY RESEARCH QUESTION

Given that computer users continue to exchange information in nanoseconds via an array of digital devices with the potential to be morphed by terrorist groups and/or other enemies into ubiquitous weapons, *what are potential users' perceptions regarding the adoptability and built-in safety of cyber-assisted olfaction technologies? What harm-reduction measures might be built-into systems that emerge from these technologies to make them more acceptable to intended users*?

Secondary Research Questions

In order to examine and discuss potential users' adoption of emergent cyber-assisted olfaction technologies, the researcher posed the following secondary questions:

1. What are the perceptions of potential users on the *adoptability* of the *MSCAO*?
2. What is the relationship between these potential users' *perceived credibility* of the *MSCAO* and their *perceived usefulness* of cyber-assisted olfactory information systems?
3. What is the relationship between the potential users' *perceived ease-of-use* of cyber-assisted olfactory information systems and their *perceived usefulness* of the *MSCAO*?

The researcher encountered many challenges during his preliminary quest for answers to these research questions. Consequently, he collected most of the

preliminary data via email communications and face-to-face conversations with experts in the areas of biotechnology, information policy, computer science and engineering, chemistry, and national security and defense. Further, he designed a survey instrument to collect complementary data from a group of engineering students.

In order to address these challenging questions, the researcher relied on expert insights, theories, concepts perspectives, and data collection and analysis techniques. More importantly, he offered a prescription against potential threats associated with emergent cyber-assisted olfaction technologies.

SIGNIFICANCE OF THE STUDY

In a *post-911* era, the significance of this research cannot be overstated. In fact, numerous reliable accounts of the use of biochemical weapons with malicious intents emerged from the literature (APPENDICES E&F). Potential adopters of emergent aroma-embedded face threats ranging from poor cyber security protocols to malicious attacks, mistaken diffusion of unwanted substances, and lack of appropriate information policies. As noted below, almost every poisonous element in the Periodic Table has been suggested at one time or another for use in warfare (Sutton and Bromley, 2005, p.270):

> Around 429-424 BC, the Spartans and their allies used noxious smoke and flame against Athens and its allied cities during the Peloponnesian Wars, and around 200 BC, the Carthaginians used mandrake root steeped in wine to sedate the Roman enemy. More recently, a variety of nerve gases, such as VX, sarin, and ricin, have been developed and used for example, by the Iraqis against Kurdish citizens in 1988, and ineffectively by a Japanese cult Aum Shinrikyo in an attack on the Tokyo subway system in 1995, which proved fatal for 12 people and injured 5500 others.

The sustained investment and deployment of emergent digital information technologies by major corporations and governments around the world have increased interest in the study of factors influencing users' adoption of emergent technologies. A good mastery of these factors is quintessential to any serious attempt to address the emergence of *techno-terrorism* in the Middle East and its inevitable mutations in various regions in the world. Since utilization of innovation diffusion theories and technology acceptance models has been proven to be effective tools to examine and explain users' adoption, the study conducted in support of the present

dissertation focused on Roger's IDT and Davis' TAM to examine the factors that positively influence potential users to adopt cyber-assisted olfaction technologies in two major categories: (1) entertainment and e-ecommerce and (2) security and safety.

Thus, as often said regarding a major biochemical attack on U.S soil, it is no longer a matter of if; it is a matter of when. Unfortunately, the same can be said about the potential Cyber-WMD threat. Hence, this dissertation offers a novel, flexible roadmap intended to assist innovators, defense and security officials, and end-users in making more informed decisions related to adoption of emergent preventive technologies.

Regarding practical applications, as previously mentioned, systems that emerge from the proposed model for cyber-assisted olfaction can be applied in aviation and mass transit security to initiate mass decontamination by dispersing an aerosolized decontaminant or to protect the public water supply against a potential bio-terrorist attack. Although many government initiatives seek to offer post-exposure remedies and various prophylactic treatments, this model is a revolutionary approach to tackle a defense and security threat dating back to the 1930's, when lethal organophosphates were introduced.

The results of this research contributed substantially to the case made in this dissertation, which focused on users' adoption of emergent technologies in order to offer a model for safer cyber-assisted olfaction to policy makers, government officials, innovators, the academic audience, and potential users.

CONCEPTUAL FRAMEWORK

Whatever the overall research assessment approach, and whatever the underlying conceptualization or models of research proposed, all investigators face a broad range of practical questions during the methodology development phase. This section outlines the design events that led to the development of the methodology, which included (1) a thorough literature review, (2) a content analysis and patent search[7], (3) a diagrammatic approach to represent the model, (4) the design of a survey instrument and the establishment of interview protocols for data collection and analysis and (5) the selection of statistical tools to assist in data interpretation. The

[7] Patent search initiated by Dr. Christopher Paradies (http:www.fowlerwhite.com). Access to these patents is also available through the U.S. Patent and Trade Office in Washington, DC.

researcher used *block-diagrams* to convey the conceptual framework of the study (Figure 1).

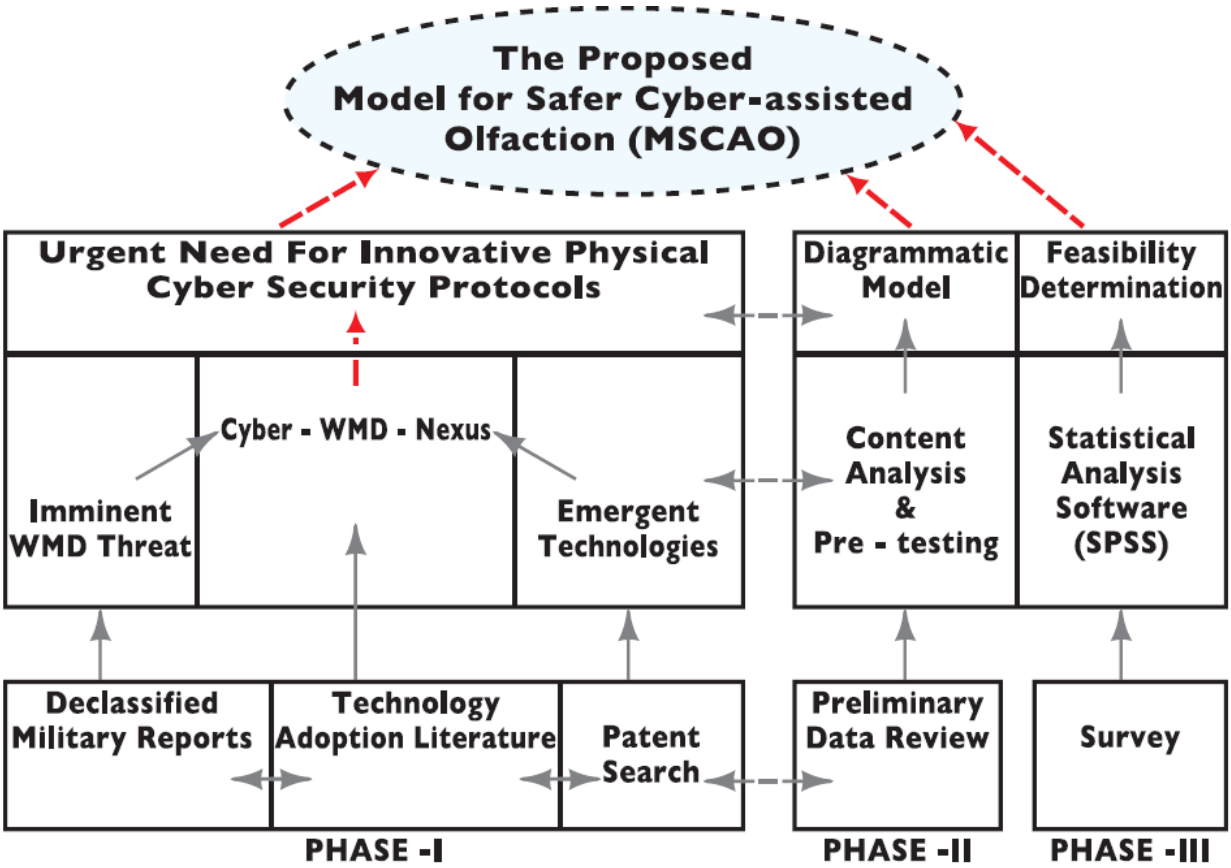


Figure 1: Conceptual framework

RESEARCH OBJECTIVES

The research objectives of this study were to:

1. Analyze *users' adoption of emergent technologies* through the recorded perceptions of a group of engineering students regarding usefulness, ease-of-use, and credibility of cyber-assisted olfaction technologies
2. Determine the *perceived credibility* of the proposed cyber-assisted olfactory information systems among these students
3. Determine the *perceived ease-of-use* of the proposed cyber-assisted olfactory information systems
4. Determine the *perceived usefulness* of the proposed cyber-assisted olfactory information systems

CHAPTER SUMMARY

This chapter covered the historical background of the proposed *MSCAO* and offered an introduction to the major concepts and themes developed throughout the entire research project. Accordingly, the objectives of the dissertation were covered, the research problem stated, the hypotheses established, research questions presented, and the significance of the study described.

Chapter 2 covers the literature review -detailing and discussing past, current, and emerging issues relevant to this research. Chapter 3 discusses mechanisms and protocols upon which the overall research methodology was built. In addition, Chapter 3 offers a diagrammatic representation of the major components of the apparatus envisioned as the very first autonomous biochemical decontaminator (ABCD) against potential threats to the ways that olfactory information could be integrated into multimodal human-computer interactions involving aroma-embedded features. The specific methods and components of data collection and analysis are also covered in Chapter 3, while Chapter 4 discusses the research findings and particularly the results of the survey instrument. Chapter 5 concludes the dissertation with recommendations and prescriptions, which amount to a fertile ground for a new, comprehensive, and flexible framework to understand various aspects of cyber-assisted olfaction technologies.

CHAPTER II: LITERATURE REVIEW

The literature reviewed in this section covers previously models of information systems, aroma-embedded information systems, social informatics, innovation diffusion theory, technology acceptance model, user perception and technology diffusion, recorded use of warfare agents, olfactory sensors/electronic noses, and their relationship to the proposed MSCAO. The researcher introduces the hypotheses and concludes the chapter with a short summary.

Preliminary data was collected at the base (e.g., declassified military reports, technology adoption literature, and patent search). Progressively, as indicated in the middle section of Figure 2 and subsequently discussed in more details, the patent search pinpointed to an emergence of cyber-olfaction technologies, whereas the military database confirmed the development of a looming biochemical threat to United States' interests at home and abroad. Since the open question remains "how" such an attack would take place within the wider context of ubiquitous information technologies, the researcher found it appropriate to explore the issue and offer useful recommendations to users, innovators, and defense and security officials (Figure 2).

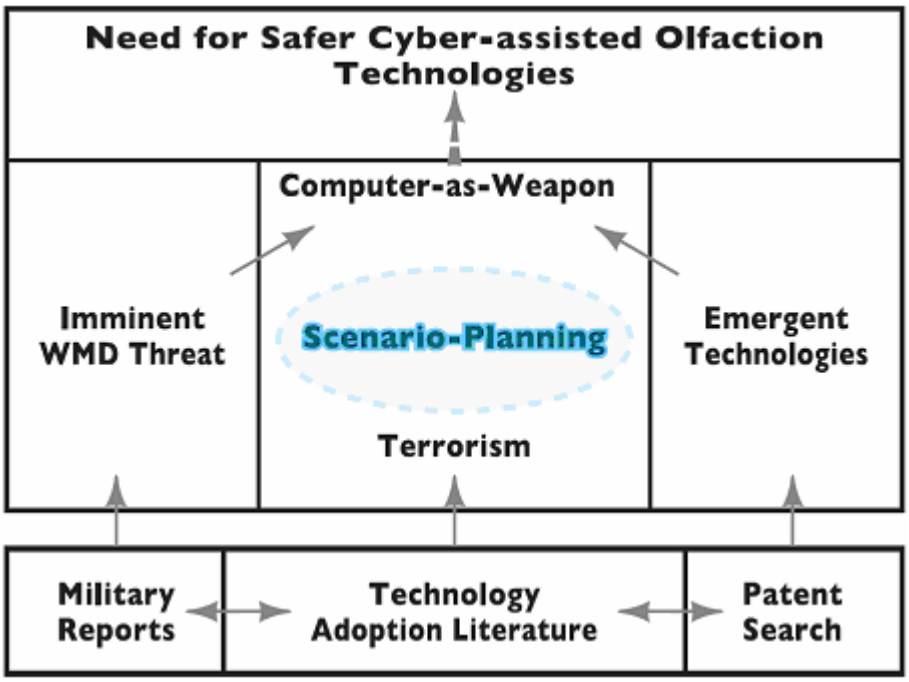


Figure 2: Convergence of Patent Search and Military Reports

Previous Models of Information Systems

The literature revealed a very long list of models aligned with Rogers' (1995) IDT and Davis' TAM. A large majority related directly to information technology (Davis, 1989; Gefen and Straub, 1997; Venkatesh, 2000; Venkatesh and Morris, 2000; McFarland and Hamilton, 2006), while others covered areas such as agriculture, business and marketing, computer simulations, economics, and medicine. For instance, Lazzaro (1989, 1991, & 1992) illustrate the suitability of certain models to represent very complex systems and processes in the field of information science and engineering.

Aroma-embedded Information Systems

Aroma-embedded information systems is a term first coined by the researcher during the 5th European Conference on Information Warfare and Security held at the National Defence College in Finland[1] to designate an information system that processes olfactory information for entertainment and e-commerce. Aroma-embedded information systems may come in many formats and embodiments.

For instance, Miwa *et al.* (2001) developed new head mechanisms and functions for a humanoid robot that has the ability to communicate naturally with a human by expressing human-like emotion. In this case, the focus was on olfactory sensation and facial color. A year later, Russell and Purnmdjaja (2002) introduced the development of complementary chemical and airflow sensing systems for a humanoid robot.

A historical review of continuous advances in human-computer interaction research revealed gradual attempts to allow machines and machine languages (e.g., avatars, robots, expert systems, neural networks, C++, and Java) to mimic, replicate, and reciprocate traditional human senses (Wiener, 1948; Brunswick, 1956; McCulloch *et al.*, 1965; Shneiderman, 1980; Taylor, 1990; Carroll, 1992; Wasserman and Faust, 1994; Watson, 1997; Fogg, 2003). Recent developments in the areas of Microfluidics and aroma-embedded information systems reiterate the prescient nature of Wiener's (1948) principles of *Cybernetics*. Cybernetics, in this context, is defined as the replication or imitation of biological control systems with the use of technology. The term itself originated in 1947 when Norbert Wiener used it to name a

[1] This conference was significant, due to the fact that Finish defense officials were gearing up to assume their role as the head (rotating presidency) of the European Union.

discipline apart from, but touching upon, such established disciplines as electrical engineering, mathematics, biology, neurophysiology, anthropology, and psychology (Wiener, 1948). The experiments conducted by Buck (1996) and Marques *et al.* (2000) shed a very bright light on the intertwining relationship that exists between human senses and aroma-embedded digital information systems.

In fact, certain fragrance cartridges use technologies similar to print cartridges for the diffusion of aromatic plumes. DigiScents, an American start-up company, promised a technology to produce thousands of different scents, triggered by software which commands a scent cartridge with 64 basic smells to mix compounds, and then send the resulting aroma wafting into a computer user's room. Although DigiScents' technology did not mature as anticipated, a recent patent search reveals a renewed interest in innovative concepts and protocols that would simplify and popularize the design and development of cyber-assisted olfaction technologies and aroma-embedded systems (APPENDIX D) using advances in Microfluidics and nano technologies (Lee, 2003; Manne, 1999; Rasouli *et al.*, 1999; Wang *et al.,* 2004).

Manne (1999) described a device which can deliver various combinations of scents in rapid succession to a user's nose in conjunction with video-graphic images and or sounds. The primary components of the device include (a) air compressor which forces air through a bank of valves, (b) a fragrance holder of compressed air which carries away the scent molecules of the gas phase (Patent # US5949522A).

Lee (2003) disclosed a fragrance emitter used with Internet. According to Lee, the fragrance emitter is able to emit various kinds of fragrance stored in vessels according to the command sent by a frequency detector which is used to search for the existence of a specific frequency specially used by a specific website (Patent# US6524537).

Rasouli *et al.* (1999) proposed an apparatus for generating odor upon electronic signal demand using a disk having an aroma-impregnated adsorbent and a substrate (Patent# US6004516).

Wang *et al.* (2004) described an information processing apparatus with an interactive scent interface to enrich users' perceptive experiences. Wang and his associates even proposed a cell phone embodiment of their aroma-embedded information system (Patent# US2004024043).

The evolution of the relationship between humans and machines (Mueller and Lazzaro, 1986) has brought the need for more human-friendly[2] intelligent systems. Many researchers are considering the possibilities to equip these intelligent systems with a certain model of human mind (a replica) in order to realize comprehensible communication with humans: the ultimate human-machine symbiosis. The technical term used among Artificial Intelligence scientists pertaining to this symbiosis is *singularity*. Metaphorically stated, singularity refers to the infusion of the human brain into an advanced computer information system. Notwithstanding certain ethical issues, aroma-embedded information is only a small piece of the ubiquitous "information pie."

Social Informatics

Social informatics is mainly concerned with the interplay between social evolution and technological innovation. Kling (2000) defines social informatics as "the body of research that examines the design uses, and consequences of information and communication technologies in ways that take into account their interaction with institutional and cultural contexts" (p. 217).

More importantly, this body of research has developed theories and findings that are pertinent to understanding the design, development, and operation of usable information systems, including computer networks, electronic forums, digital libraries, and electronic journals (p. 218). Some of the key themes include the importance of social contexts and work processes, socio-technological networks, public access to information, and virtual communities. Rob Kling was an authoritative voice on this subject. Other relevant discussions are held in (Kling *et al.*, 1998; Dutton 1997; Kiesler, 1997). Innovation diffusion is relevant to the interplay between computers and society. As emerging cell phone and Internet applications suggest, cyber-assisted olfactory information exchanges may involve a social event. As such, the social informatics literature is very relevant to the current discussion.

Innovation Diffusion Theory (IDT)

Diffusion theory models the dynamics of technology adoptions, including the rate of adoption and the eventual spread of innovation in a social system (Short *et*

[2] Human-friendly is used in place of user-friendly to acknowledge the fact that other species (even certain robots) are interacting with intelligent systems as "users." For example, an animal can be trained to break an infrared spectrum in order to activate a water dispenser. Another example is 'robots building other robots.'

al., 1978; Schneiderman, 1997). A new technology (or innovation) is often introduced in a social group (community, organization, nation, market, or an industry) by a change agent with an interest to promote it (private firm, public agency, or other interest groups). Typically a few actors are the first or early adopters; the success of the innovation often depends on their social status or influence. Other members of the group, who are either directly acquainted with, or share similar interests with the early adopters, may be persuaded to adopt the innovation, and they in turn influence others. This is a real techno-psycho-sociological exercise. In fact, successive waves of adoption continue until the innovation reaches a saturation point or *ceiling* that varies depending on the characteristics of the innovation and the social system. Important concepts of diffusion include the adoption *threshold,* the number of adopters necessary to induce one more actor to adopt an innovation (Rogers, 1995; Davis, 1989), and *critical mass,* the point at which enough actors have adopted an innovation for it to succeed, based on the rate or momentum of adoption (Tornatzky and Fleischer, 1990; Basu *et al.*, 1992; Boahene, 1995).

In this study, the researcher used a multi-scale evaluation instrument based on Rogers' (1995) IDT. Rogers proposes that five attributes of an innovation influence its acceptance. These attributes are in accord with the present research protocols and have been operationalized in previous surveys to evaluate a variety of communication systems and information technologies (Gefen and Straub, 1997; Venkatesh, 2000; Legris, Ingham, and Collerette, 2003; Venkatesh and Morris, 2000). Rogers' five attributes (relative advantage, compatibility, complexity, trialability, and observability) are based on users' intention to adopt a particular technology. According to Rogers (1995), "these are perceived attributes that emerged from the meta-theory that includes innovation, type of innovation decision, communication channels, nature of the social system and the change agents" (p. 207). As the literature review suggests, these attributes are applicable in domains such as biomedical engineering, computer models, and airline reservation information systems (Rogers, 1995; Tornatzky and Fleischer, 1990; Bero *et al.*, 1998).

Technology Acceptance Model (TAM)

TAM was developed by Davis (1989) to explain computer-usage behavior. The theoretical basis of the model was Fishbein and Ajzen's (1975) Theory of Reasoned

Action (TRA). The original goal of the TAM was "to provide an explanation of the determinants of computer acceptance that is general, capable of explaining user behavior across a broad range of end-user computing technologies and user populations, while at the same time being both parsimonious and theoretically justified" (Davis *et al.*, 1989, p. 985). TAM is widely used across many disciplines (Keil *et al.*, 1995; Satzinger and Olfman, 1995; Taylor and Todd, 1995; Igbaria *et al.*, 1996) to examine users' intent to adopt a particular technology. Davis (1989) suggested that acceptance or usage was determined by two factors: perceived Usefulness and perceived Ease-of-Use (Figure 5). Although TAM focused primarily on usefulness and ease-of-use, Kelman's (1958) early study of social influence was motivated by his interest in understanding the changes brought about in individuals' attitude by external inputs, such as information communicated to them. Specifically, his research attempted to understand if the change in attitude resulting from external stimuli was a temporary superficial change or a more lasting change that became integrated in the person's value system.

In effect, the geospatial popularity and cross-cultural applications of TAM to explore users' adoption of emergent technologies can not be denied (Straub *et al.*, 1997). TAM has been applied directly, extended, or simply used as a supportive theoretical framework to examine users' adoption of existing and emergent technologies in the United Kingdom (Al-Gahtani, 2001), the European Union (Brown *et al.,* 2002b), Malaysia (Ndubisi and Jantan, 2003), the Americas (McCoy *et al.*, 2005), China (Chan and Lu, 2004), and in the United States (Davis, 1989; Jaeger, 2005).

Notably, the literature also revealed the adoption of TAM in variety of disciplines, such as decisions sciences (Venkatesh and Davis, 1996; Lucas and Spitler, 1999; Lederer *et al.*, 2000), telemedicine (Chau and Hu, 2002), management science (Bass, 1969; Kim and Malhotra, 2005; Szajna, 1996; Davis, 1989; Taylor and Todd, 1995), library information systems and documentation (Spacey *et al.*, 2004; Jaeger, 2005, Lin and Lu, 2001; Ingwersen, 1996), and information systems (Brown *et al.*, 2002; Wang and Benbasat, 2005).

Martins and Kellermanns (2001) used a combination of the technology acceptance model (TAM) with literature on change management to develop and test a model predicting user acceptance of a new Web-based information system.

Martins and Kellermanns found that “the change enablers predict perceived ease of use, whereas the change motivators predict perceived usefulness of the system. Perceived usefulness and ease of use predict attitude toward the system, which in turn predicts behavioral intention to use the system, which predicts use of the system” (p. 607).

Lin and Lu (2001) addressed why users accept or reject a Web site and how user's acceptance is affected by the features (i.e. information quality of a Web site, response time and system accessibility) provided by a Web site. The results showed that the technology acceptance model (TAM) fully mediated the usage behavior even in the Internet environment, accounting for 64% of the variance in usage.

Jaeger (2005) built on Grandon and Pearson’s (2004) use of TAM (for the exploration of the acceptance of e-commerce by small and medium sized businesses as a part of their business activities) to examine how United States federal government agencies comply with the standards relating to accessible websites for people with disabilities. In particular, Jaeger (2005, p.20) discussed the establishment of a conceptual framework based on the idea of a modified TAM for organizational acceptance of new technology.

Nonetheless, it is important to note that, contrary to much existing research on TAM that has observed expected usage to be a reliable predictor of future actual use of technology, some researchers (Melone, 1990; Schewe, 1976) have argued that observed behavior may not always be consistent with underlying psychological dispositions.

User Perception and Technology Diffusion

The utilization of users’ perception to evaluate system design and feasibility is not new (Bondonio,1998). In fact, it was used in the early 1980’s by information system researchers with vendor organizations such as IBM (Gould and Lewis, 1985) and Xeros (Bewley *et al.*, 1983).

For instance, in the biomedical arena, if respected and influential clinicians argue for and demonstrate the application of a new procedure or treatment approach, it is likely to have a positive impact upon adoption rate (Bero *et al.*, 1998). The more charismatic the person providing the role model, the greater the chance that a larger number of other professionals will adopt the advocated change in clinical behavior. In surgery, new techniques are often adopted very quickly, as there is a common

perception that there are disadvantages in being “left behind” by not adopting the new technology (Denis *et al.*, 2002). This phenomenon is explained by Rogers in terms of *observability*: the degree to which the results of the innovation are visible to others. Evidently, observability is a trait of user perception.

Since instrument validity is very often supported by a theoretical framework (Anastasi, 1986), the researcher uses Rogers’ (1995) IDT to validate the design of the survey instrument, which serves as a source for data collection, analysis, and interpretation. Relative advantage is a key concept of Rogers’ theory. According to Rogers, relative advantage is the degree to which a new innovation surpasses current practices. Relative advantage can be operationalized, or measured, in terms of variables such as usefulness in accomplishing work goals, quality of work outcomes, added convenience and social prestige provided by the innovation. Rogers’ (1995) diffusion theory has been very useful in the design of the survey instrument. In particular, the researcher uses Rogers’ attributes as a theoretical foundation to develop his own constructs in order to evaluate the feasibility of the proposed *MSCAO*, based on the respondents’ perceived usefulness, ease-of-use, and credibility. Accordingly, the researcher selected these four perception-based constructs (mentioned above) to design the survey instrument and structure the interview protocols. Subsequent discussions will cover these constructs in more details. The *MSCAO* is primarily based on the diffusion of biochemical particles (aromas and decontaminants). Multimedia applications have been mainly limited to the use of audiovisual information, stimulating two of the five senses of human beings. The MSCAO could bring an important support to advance in fields like distance education, military, telemedicine, and entertainment in the near future.

KEY CONCEPTS

Recorded Use of Warfare Agents

Airborne chemical and biological warfare attacks against human subjects often target the cholinergic and glutamatergic receptors. These receptors fulfill an important function in the central nervous system. They are also closely connected with the respiratory system. In this area, the literature offered ample details concerning the evaluation of binding sites and the mechanism of action of cholinesterase inhibitors (Quinn *et al.*, 1995; Radić *et al.*, 1991; Reiner *et al.*, 2000). Biochemical warfare agents tend to further complicate malicious asymmetrical

warfare practices with the additional mass casualty factor. The potential integration of information technologies could exponentially degenerate this (already) mismanaged global proliferation of biochemical warfare agents. For instance, Grabow (1991), Torrens (1999), and Anderson (2001) discussed biochemical threats from a military perspective, while Aas (2003) focused medical management of nerve agent intoxication with several recommendations for propositions for prophylactic countermeasures.

Malicious attempts also account for terrorist acts and other deliberate attempts by other enemies to use WMD to tamper with digital information technologies (Hyacinthe, 2006c). In the context of an aroma-embedded information system, any attempt to tamper with chemical capsules or their intended purposes would be considered malicious (if not criminal). Numerous reliable accounts of the use of chemical weapons with malicious intents are reported in his dissertation. The search for protection against biochemical warfare agents has been very persistent.[3] For instance, Sutton and Bromley (2005) described a variety of technologies that can be used to fight biochemical warfare agents. They also put special emphasis on scanning mechanisms to detect explosive materials. Moreover, Singh and Singh (2003) and Sutton and Bromley (2005), particularly addressed the biochemical threat that looms over aviation and mass transit of major metropolitan cities around the world.

According to Sutton and Bromley (2005),

> Biological weapons have a long history both in warfare and in terrorism. The most important biological agents (they noted) are smallpox, caused by a virus (*Variola mjor*); anthrax, caused by a bacterium (*Bacillus anthracis*); and plague, caused by a bacterium (*Yersinia pestis*). Over 53 biological agents are identified as potential biological weapons (p. 272). The smallpox incident in Britain illustrates the danger posed by this type of error. "...the British experienced some difficulties and a very small release of their virus resulted in several deaths but these were contained and the virus did not spread further" (p. 273).

[3] Meselson, M. (2001). Bioterror: What Can Be Done? *The New York Review of Books*. Available: http://www.nybooks.com/articles/14971; Henderson, D.A. (1999). The Looming Threat of Bioterrorism, *Science, (283*), 540, 1279-1282; Miller, J., Engelberg, S., and Broad, W. (2001). The Future. In *Germs: biological weapons and America's secret war (pp. 287-31)*. Simon and Schuster.

Unclassified and declassified military reports offer an in-depth coverage of the biochemical threats by experts and military scholars from the U.S. Navy, the Army, the Marine Corps, and the Air Force (McCoy, 1999; Grabow, 1991; Torrens, 1999; Anderson, 2001; Webb, 1999).

According to Lt. Col. Linda Torrens (1999, p.v) of the U.S. Air Force, "WMD terrorism will play a larger role in this new uncertain security environment for several reasons. First, transnational threats are no longer kept in check by a bipolar world. Secondly, terrorists may have greater access to WMD materials today than ever before. And thirdly, the information revolution has made not only weaponization knowledge freely available, but has also improved the organizational capabilities of diverse terrorist groups." Torrens further noted the potential for greater losses in the case of a WMD attack, using such agents as small pox virus (Stuckey-French, 2001; Hull, *et al.*, 2003).

In spite of the development of very sensitive biosensors, post-exposure remedies would still leave occupants of aircrafts, military installations, and mass transit vehicles very vulnerable. Moreover, traditional prophylactic treatments are largely limited to the military, emergency rescue personnel, and other authorities (Hyacinthe, 2005b). Simply put, responses to the biochemical threat so far have been restricted to prophylaxis and therapy, with human subject as the primary target (Malcolm, 2001; Russell *et al.*, 2003). Unfortunately, the complex genetic profile of the *Homo sapiens*, the sophisticated nature of the central nervous system, and the intricacy of the human respiratory functions will continue to pose insurmountable challenges to any attempt to apply a "silver bullet" antidote.

There is an obvious lack of resources and expertise vested in the neutralization of warfare agents *per se*. Instead, attention has been focused on *detect-to-warn* systems and on practices such as post-exposure, therapeutic treatments. Detect-to-warn systems are primarily based on biochemical sensors that scan the horizon, bodies of water, and the soil for bioactive substances. Several techniques are currently available to improve detection. The choice of a particular technique often depends on the target, type of the threat, and availability of the appropriate technology. Although biosensors often relate to detection systems that are based on enzymes or bio-affinity, biochemical sensors and biosensors are used

interchangeably in this paper to explore the detection of chemical and biological agents.

Renaudin *et al*. (2004) discussed surface acoustic wave (SAW), another detection technique commonly used by bio-defense experts (Frye-Mason *et al*., 2000). In sum, various light-scattering techniques may be used to detect and digitally encode these agent-specific information signatures (Figure 3). The figure below illustrates a common detection technique that uses scattered beams to identify a particular molecule. Observation is made on the right (microscopic objective).

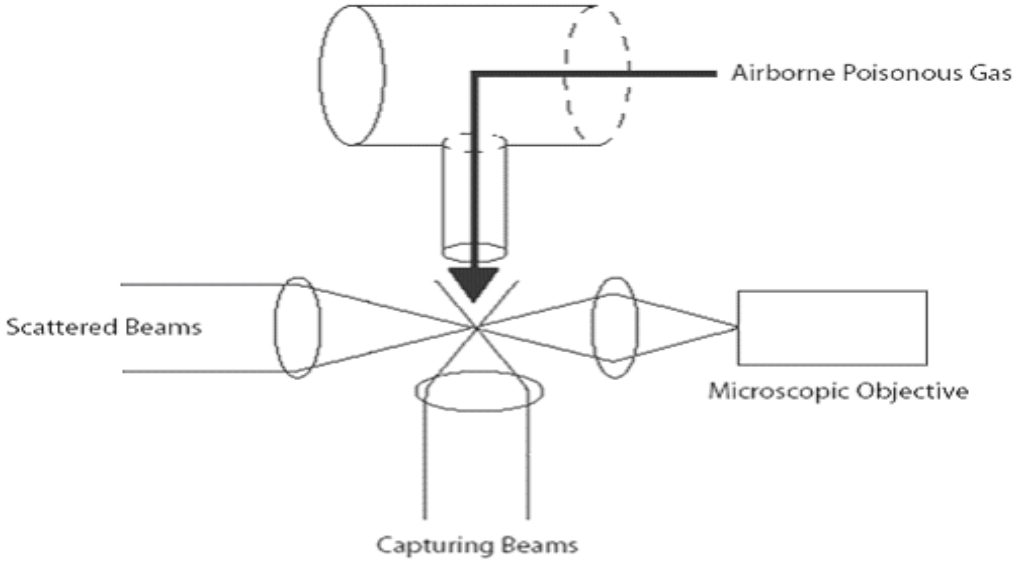


Figure 3: Light-scattering detection technique

Olfactory Sensors/ Electronic Noses

Essentially, "e-noses" mimic the sense of smell. Consisting of olfactory sensors and a suitable signal-processing unit, they are able to detect and distinguish odors precisely and at low cost. Hence, a basic description of the autonomous biochemical decontaminator would reveal an e-nose attached to an automatic decontaminant dispenser (Figure 3 and Figure 8). Some e-noses are also known as *biosensors*.

Biosensors are widely used to detect biological, pharmacological, or clinically important compounds. That is one reason why enzyme biosensors have to be selective and very sensitive. In addition, these biosensors are often portable and easy to use. Because enzymatic biosensors can detect only those substances of interest and ignore all other environmental and biological interferences, other detection technologies may be used in parallel to widen the detection spectrum of

certain mission critical chemical warfare monitoring systems. The proposed autonomous biochemical decontamination system primarily targets biochemical warfare agents, not the exposed subjects *per se*. In short, the *threat* is targeted, not the potential *victims*.

In summary, Microfluidics and μTAS technologies, which move microscopic and nano-scale drops of fluid, are crossing new frontiers in the realms of real-time enzymatic analysis, DNA analysis, and proteomic analysis involving proteins and peptides (Chatterjee *et al*., 2005; Fair *et al.*, 2004; Frye-Mason *et al*., 2000; Nelson *et al.*, 2000; Fei *et al*., 2006). Some of the common applications include high-throughput screening of drug candidates and point-of-care testing. The distinct advantages that they bestow on applications are pushing LoC technologies from R&D to commercialization at a very rapid pace. As previously indicated, biosensors are becoming relatively inexpensive and portable. However, as the deployment of Microfluidics-based biochips progresses, their widespread use is expected in the areas of cyber-assisted olfaction to enhance technologies such as scented emails and other aroma-embedded information technologies. Among many other applications, implanted drug delivery systems, remote drug administration, and biochemical warfare will further sophisticate the diffusion of this emerging technology. The potential misuse of these technologies to engage in *cyber-assisted olfactory information warfare* is a major concern in this dissertation.

Information Warfare

The emergence of information warfare (IW) as a driving force behind the spread of global terrorism clearly shatters the conventional wisdom that purports IW as a sophisticated proprietary intelligence/military strategy of the world's superpowers to attain and maintain information superiority through the disruption of adversary information, information systems, and computer processes and networks, while protecting their own information infrastructure; instead, IW proves to be an effective, flexible, and affordable intelligence tool (Hyacinthe, 2006; Libicki, 1995; Toffler and Toffler, 1993). IW practitioners rely on sensors from spectra such as infrared, ultraviolet, olfactory, auditory, visual, seismic, and others in the fight to obtain and sustain information superiority. Nonetheless, it is safe to suggest in the case of a computer-based IW campaign, information collection is much less dangerous and

much more rapid because avatars and human agents can concurrently infiltrate and gather accurate information with lesser collateral damages (Hyacinthe, 2005a).

The concept of IW is not new. From the exploration of domestic threats against America's homeland by Morgan (2003) to review of strategies and tactics by Bishop and Goldman (2003) and Coffman *et al*. (2004), investigators of various disciplines have turned and remained tuned to this emergent battle strategy. As the literature suggests, a holistic, comprehensive approach will be necessary in order to secure the most critical information infrastructures and maintain a respectable margin of information superiority (Sharma and Gupta, 2002; Molander, 1996; Libicki, 1995).

Libicki (1995) separated seven different forms of IW: (1) command-and-control warfare, (2) intelligence-based warfare, (3) electronic warfare, (4) psychological warfare, (5) hacker warfare, (6) economic information warfare and (7) cyber warfare. However, after reviewing these seven forms of IW (and accounting for recent terrorist mutations), the researcher responded with a cyber warfare design wherein, cyber-assisted olfactory information warfare plays an important role. The paradigm of olfactory information warfare emerges from Libicki's multiple perspectives, making IW a relevant component of this dissertation.

PRAGMATIC APPROACH TO LESSONS LEARNED

Lethal mutation refers to the seamless fusion of digital information technologies with weapon systems to produce the deadliest weapon arsenals of the future while *technology-defense singularity* purports that the fusion of emerging digital technologies with next-generation weapon systems would deliver and protect society against the most lethal weapons. The researcher characterized it as multispectral, widespread, and potentially dreadful. In fact, a quick review of the progressive use of computers as offensive weapons reveals an evolution from human assistants in building complex algorithms (e.g., launch precision-guided missiles) to active components in bomb making (e.g., timing and sensing) to semi or fully autonomous unmanned aerial vehicles (UAVs) for military operations. In this context, a UAV is considered as a multipurpose flying computer that serves simultaneously as pilot, gunner, dispatcher, missile launcher, missile defense shield, and more. DARPA has shown great interests in the development of micro and nano air vehicles also known as NAVs. John A. Main of DARPA manages a program that

involves NAV platforms with the revolutionary ability to fly under very difficult conditions, navigate in complex environments, and communicate over significant distances (DARPA, 2007; O'Neill, 2006).The NAVs may soon collaborate with human agents in emergency rescue and urban warfare operations as components of evolving network centric operations (NCOs). With advances in microfluidics and micro total analysis systems (μTAS), many more applications are being considered.

Though applications associated with the *technology-weapon singularity* cited above may evolve with time and new scientific discoveries, the underlying principles of this singularity are not new. For instance, Edwards (1996) noted that "…by almost any measure –scale, expense, technical complexity, or influence on future developments—the single most important computer project of the postwar decade was MIT's Whirlwind and its offspring, the SAGE computerized air defense system" (p. 75). Smart defense weapon systems often involve embedding high-performance computing inside traditional weapons with one or more sensors. In fact, new classes of smart defense systems are emerging. Against biochemical threats, as the literature suggests, computers facilitated advances in biosensor technologies that allow the detection of biochemical, high yield explosives, and nuclear and radio active materials with higher precision and shorter delays (Collings and Caruso, 1997; Preston and McFadden, 2001; Mayzner and Dolan, 1978; Srinivasan *et al.,* 2003). In addition, computers have facilitated the design and implementation of digital solutions to many problems and many threats (e.g., conventional and unconventional). As such, the researcher envisaged a combination of smart biosensors and effective cyber-assisted harm-reduction measures (e.g., suppression and/or neutralization) to support his proposed MSCAO.

HYPOTHESES

Potential adopters of emergent cyber-assisted olfaction technologies are more likely to find the *MSCAO* acceptable if their "perceived usefulness" and "perceived ease-of-use" of these technologies are significantly high and their "perceived credibility" of the harm-reduction and security measures proposed in the *MSCAO* is also significantly high (Figure 4).

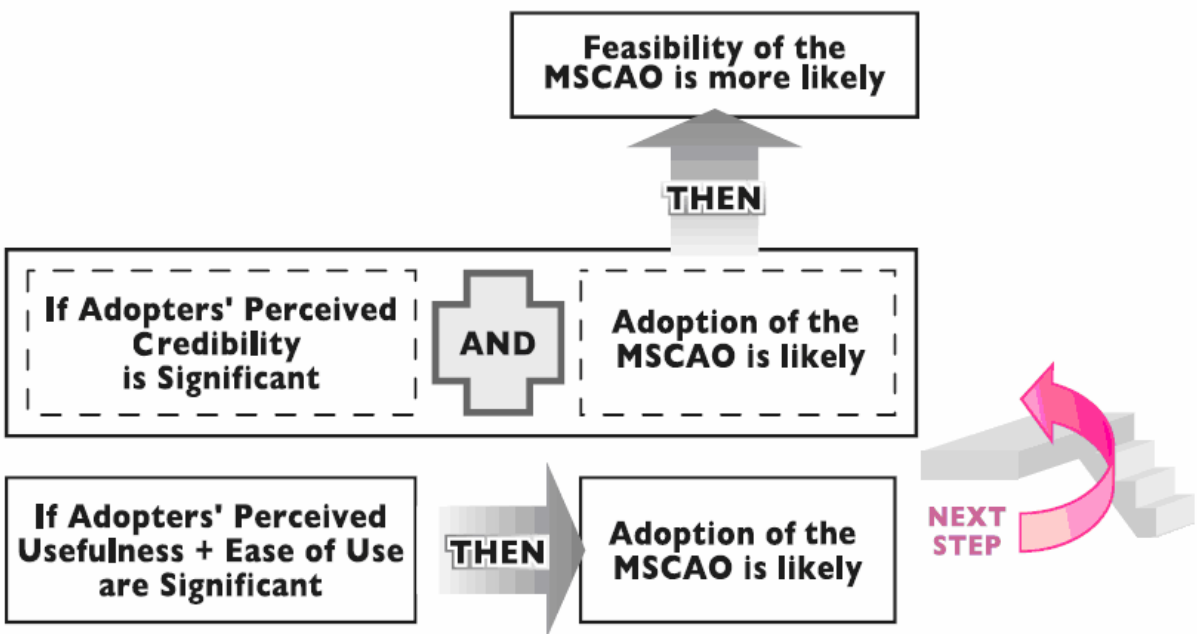


Figure 4: Primary hypothesis illustrated

Hypothesis 1 (H_1)**:** *"Perceived Usefulness" and "Perceived Ease-of-use" are positively correlated to likely adoption of the MSCAO;*

Hypothesis 2 (H_2)**:** *"Perceived Usefulness" is positively correlated to "Perceived Credibility" with regards to the likely adoption of the MSCAO;*

Hypothesis 3 (H_3)**:** *"Perceived Usefulness" is more important than "Perceived Ease-of-Use" when considering the likely adoption of the MSCAO;*

Hypothesis 4 (H_4)**:** *"Perceived Credibility" is more important than "Perceive Ease-of-Use" when considering the likely adoption of the MSCAO;*

Hypothesis 5 (H_5)**:** *Electrical engineering students display a more positive attitude toward the credibility of the MSCAO than electronic engineering students.*

CHAPTER SUMMARY

The foregoing discussions covered previous research relevant to this dissertation. The documents reviewed included various academic publications, patent searches, and declassified military reports. In particular, the researcher discussed key concepts and theories associated with users' adoption of emergent technologies. He established the relevance of previous literature covering airborne

warfare agents to the ongoing quest for harm-reduction measures against emerging threats to cyber-assisted olfactory information exchanges in a variety of settings.

This chapter captured the reviewed literature according to the researcher's interdisciplinary approach to information science. According to a similar approach, Capurro and Hjørland (2003) described information science as a multidisciplinary science with the support of Marijuan (1996, p. 91) who identified information science as a putative vertical science, which "…creates its own spattering of subdisciplines in the overlapping with the other existing sciences: information physics, information chemistry [molecular computing], bioinformation [artificial life], informational neuroscience [artificial intelligence], and socioinformation."

In addition, the researcher reviewed references that seem to extend the traditional definition of "information." In bioinformatics, for instance, cell communication expert, Loewenstein (1999) observed that it is not energy that counts in biological systems, but *information* (p. 58). He further suggested that biological systems can be treated as networks in which information exchanges occur. Thus, the researcher approached cyber-assisted olfactory information exchanges with a natural affinity to Capurro's multidisciplinary paradigm and Loewenstein's extension of the concept of information to cellular biology. As the literature further revealed, cyber-assisted olfaction may involve biochemical transactions both in detection and inhalation of airborne particles (Sutton and Bromley, 2005; Loewenstein, 1999; Wang *et al.,* 2004; Hyacinthe, 2006a; Hyacinthe and Anglade, 2007).

This research is drawn on a number of seemingly distant disciplines to offer a rich, comprehensive, and original theoretical framework to study aroma-embedded information systems and to counter the potential dangers associated with the implementation of such systems. More importantly, it prescribes several mitigating solutions against the identified threats.

In sum, through this chapter, the researcher established the relevance of the documents reviewed (Davis, 1989; Grabow, 1991; Rogers, 1995; Manne, 1999; McCoy, 1999; Rasouli *et al.*, 1999; Torrens, 1999; Webb, 1999; Anderson, 2001; Lee, 2003; Singh and Singh, 2003; Wang *et al.,* 2004; Sutton and Bromley, 2005) to his research objectives. Before concluding this chapter, the researcher also introduced the five hypotheses, which will be discussed further in Chapter 4.

CHAPTER III: RESEARCH METHODOLOGY

CONCEPTUAL DESIGN, RATIONALE, AND METHODS

This chapter covers the methodology for collecting data with the goal of testing the hypotheses discussed below. It discusses the chosen set of methods, the reasons for making the choice of action research, and the particular type of action research found most relevant. Further, the researcher covers standard and micro representations of the *MSCAO*, along with various anticipated applications. Prior to a brief section summarizing the objectives attained, the chapter discusses how the researcher conducted the survey and how the scenarios were presented to the respondents.

CONCEPTUAL DESIGN

The study utilized qualitative and quantitative research methodologies to collect data utilized to answer each of the research questions (Cresswell, 2002). Close attention was given to the way terminology was presented throughout the dissertation in both written and spoken forms between the researcher, participants, and readers, to ensure that key terms are clearly explained and understood. In a continuous effort to maintain clarity, wherever field specific jargon was absolutely necessary, the researcher provided a platform of shared symbols, according to guidelines established by Hutchins and Hazlehurst (1995), to facilitate his interaction with the audience. The researcher went through three phases according his original research agenda.

Phase I: Data Collection via Plurality of Data Sources

In many aspects, this research is atypical, for it covers two intertwining, yet very distinct and controversial aspects of information technologies applied to global security and defense: (1) the exposition of a hidden cyber-WMD nexus and (2) the presentation of a model to mitigate the dreadful effects of such threat. To address this problematic, twofold issue, a plurality of sources was needed. As previously noted, argumentation regarding the cyber-WMD nexus will be substantiated with a comparative content analysis (Weber, 1985) of a series of technical reports from U.S. military experts addressing biochemical warfare and terrorism, graduate and post-graduate military theses, and research articles in the areas of national security and defense against weapons of mass destruction, asymmetrical warfare, and emergency rescue operations (Hyacinthe, 2005b).

Phase II: Content Analysis

Content analysis is a technique for drawing inferences from existing records or documents in a systematic and unbiased way. Its advantages include the availability of large populations and the possibility to document naturally occurring trends over time. Nonetheless, the data collection is very difficult to manage. Weber (1985) provides detailed information on this particular research technique.

Particular attention is directed towards aroma-embedded information systems, Microfluidics, detection and decontamination of olfactory information systems.

Phase III: Emergence of the MSCAO through interpretation of results

To explore the perceptions of potential adopters of the proposed MSCAO, this study used a mixed-methods approach (Mingers and Gill, 1997). According to results obtained (e.g., sedimentation of the literature review, comparative analyses of patent searches and military reports, informal interviews with TAM scholars and security experts, and the survey instrument), the researcher concluded that the development of olfactory devices by security/safety minded engineers, along with significant progress in understanding the users' intentions to adopt emergent digital information technologies may offer tremendous opportunities for building safe multimedia applications, which will stimulate the sense of smell in multimodal human-computer interactions.

RATIONALE

The researcher implemented a mixed-methods data gathering technique. Qualitative and quantitative research methods were used because each has unique and distinct advantages to answer the research questions posed. The mixed-methods approach to data gathering allowed the researcher to perform multi-dimensional analyses of the information collected regarding users' adoption of emergent cyber-assisted olfaction technologies.

As part of the administrative procedures, the Florida State University Human Subjects Committee (APPENDIX A) approved this study and the researcher employed a survey instrument as his primary data collection tool. The researcher obtained a separate clearance for students matriculated at the Florida A&M University (APPENDIX B). In addition, given that the survey method ordinarily portrays one side of a sophisticated picture, the survey data was complemented by a comparative content analysis and informal interviews with experts in the areas of

national defense, biochemical warfare, and emerging aroma-embedded information systems. The latter activities allowed for qualitative data collection that were quantified in order to determine causality between constructs (e.g., “how” and “why” certain choices were made). The *MSCAO* is based on the theoretical constructs of behavior applied to the specific context of technology adoption. Davis’ (1989) technology acceptance model (TAM) was very instrumental in the overall design of the methodology (Figure 5). According to the literature, perceived usefulness has proven to be the strongest of the two TAM variables, with perceived ease-of-use having mixed and inconclusive results (Keil *et al.*, 1995; Satzinger and Olfman, 1995; Taylor and Todd, 1995; Igbaria *et al.*, 1996).

For each measure, standard items were adapted to the context (users’ adoption of cyber-assisted olfaction technologies) of the study. The choice of credibility as a perceived attribute of emergent technologies is unique to the proposed model. The term credibility has been used in social psychology to refer to individuals’ general ability to express their perception related to trust and security (Fogg, 2003; Van der Heijden *et al*., 2003). The researcher also introduced “credibility” as an *extended TAM* construct based on previous combinations of TAM with “trust” (Gefen *et al.,* 2003; Wang and Benbasat, 2005).

The traditional TAM includes four concepts: ease-of-use, usefulness, attitudes towards use and intention to use (Figure 5). It is important to note that early adopters of emergent technologies are likely to be in their youth. They expect challenging (not-so-easy-to-use) technologies to match their advanced computer skills. More people than ever are becoming early adopters of technology (Waters, 2007).

In this dissertation, the survey instrument served as the basis for a major part of the data analysis performed during the researcher’s exploration of users’ adoption of emergent technologies. It also served as a tremendous support to the overall research initiative. According to Figure 5, socio-technological interactions (*external variables*) affect how users *perceived usefulness* and *perceived ease-of-use* of a particular technology. The diagrams also show that *perceived ease-of-use* influences *perceived usefulness*. A closer look at the diagrams also shows that *perceived usefulness* and *perceived ease-of-use* influence *attitude towards using*, which in turn affects *behavioral intention to use* (Jackson *et al*., 1997; Luarn and Lin, 2005). Lastly, on the far-right, Davis (1989) suggested that the latter factors may be used to anticipate *actual system use*.

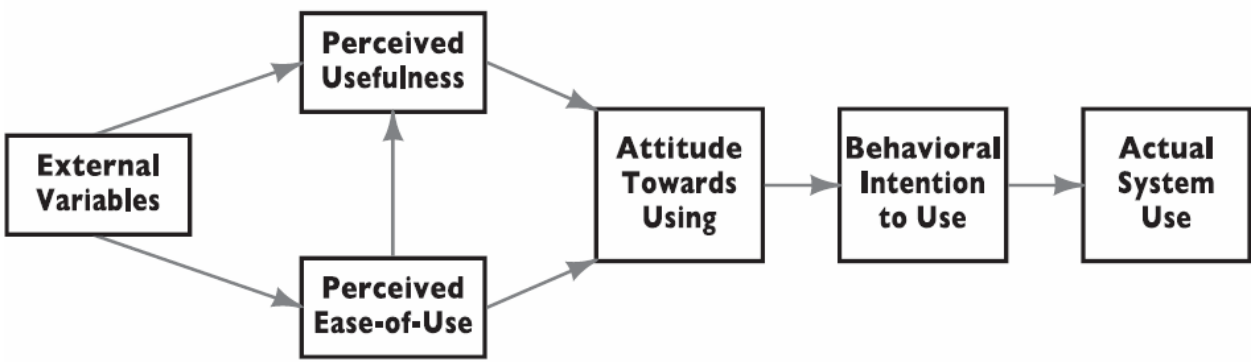


Figure 5: Davis' (1989) Technology Adoption Model

PREVIOUS MODELS OF INFORMATION SYSTEM

The researcher sought to take advantage of both quantitative and qualitative data collection methods, which provided useful clues on the participants' perceived feasibility of the proposed cyber-assisted olfaction technologies (particularly aroma-embedded information systems). Accordingly, four constructs (usefulness, ease-of-use, and credibility) were carefully formulated from Rogers' (1995) innovation diffusion attributes, Davis' (1989) perception-based scales for technology acceptance, and Fogg's (2003) web credibility model, in order to determine the levels of influence of these constructs on the adoptability of the proposed MSCAO. As indicated in earlier discussions, the proposed system is represented by a diagrammatic domain model: a model that encapsulates several of the six models suggested in (Davies *et al.*, 2005).

In fact, built primarily on prior models (Lavis *et al.*, 2003; Weiss, 1979; Hanney, 2002), Davies *et al.* (2005) suggested the following taxonomy:

1. Classic, knowledge-driven model: a linear view that research findings may be communicated to impel action.

2. Problem-solving, policy-driven model: a second linear view that begins with the end-users of research and the problems they face, before tracking back in search of useful findings.

3. Interactive model: here the process is modeled as a set of (non-linear, less predictable) interactions between researchers and users, with research impact happening through complex social processes of 'sustained interactivity.

4. Enlightenment model: this model eschews the notion that research impacts are simple and instrumental in effect; instead research is seen to impact through 'the gradual sedimentation of insight, theories, concepts and perspectives.

5. Political model: here research findings are seen to impact adversarial systems of decision making.

6. *Tactical model: in this model, research becomes a resource to be drawn on whenever there is pressure for action on complex public issues, and may be used not just to bolster decision making but also to stall and deflect pressure for action.*

After a careful review of these models, the researcher found the first two to be the most relevant to this study. First, according to the classification scheme presented by Davies *et al.* (2005), the present model falls under the classical, knowledge-driven type. In fact, it seeks to *impel action* (securing and safeguarding aroma-embedded information systems), based on the researcher's findings related to users' perceived acceptability of the MSCAO. Second, the present model relates to *problem-solving and policy-driven*, for it touches on information policies and security/safety protocols associated with olfactory information exchanges. This relationship is manifested by the attempt to address the cyber-WMD threat (i.e., the problem solving aspect). However, the researcher's affinity with the fourth model listed above is evident. For example, the convergence of the findings is inline with the "gradual sedimentation" concept of the enlightenment model.

Thus, *modeling* was determined to be an appropriate tool for this research. A survey questionnaire (APPENDIX C) was designed to determine how much influence the selected variables would have on the respondents' intention to adopt the proposed model. As illustrated on Figure 6 below, the thicker the arrow, the higher the recorded influence of the selected variables on adoption.

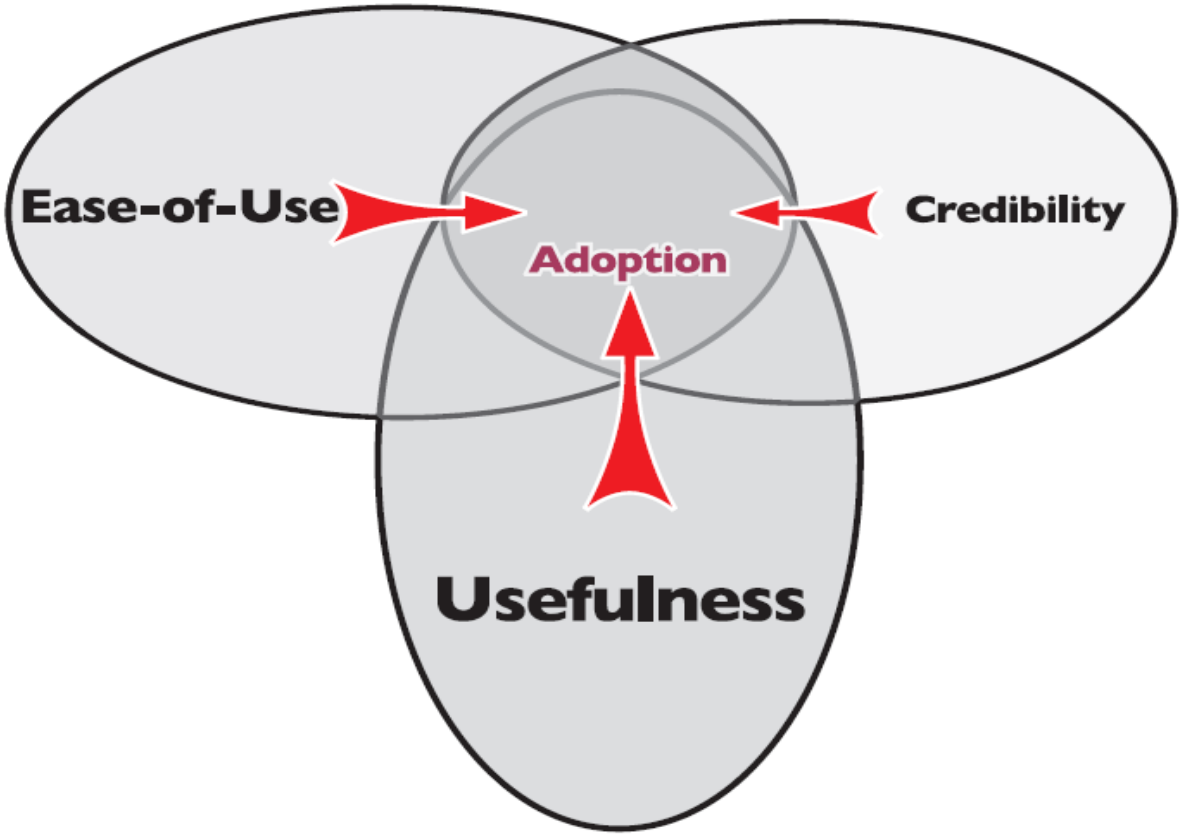


Figure 6: Influential relationships between constructs

BLOCK-DIAGRAMS

In this section, the researcher presents the main components and illustrates the primary features of the proposed *MSCAO* using *block-diagrams*. Either representational or computational metaphors can be utilized in the representation of visual mental images. These images play an important role on how users perceive usefulness, acceptability, and robustness of an emergent technology (Davis, 1984). A scientific correlation has been established between cognitive mechanisms involving inspection of diagrams and those involved in the creation of mental images and decision-making (Kosslyn and Sussman, 1995). As for an assessment of how much retention occurs with diagrammatic representations, Nobre *et al.* (2004) pointed to a high level of compatibility of diagrammatic representations to the cognitive mechanisms of working memory. In addition, Carley (1996) explored the potential of information technology to communicate new ideas. Several models have been introduced in Chapter 2 and their use further discussed in this chapter. The researcher utilized seven cases to introduce the MSCAO concept. Each case

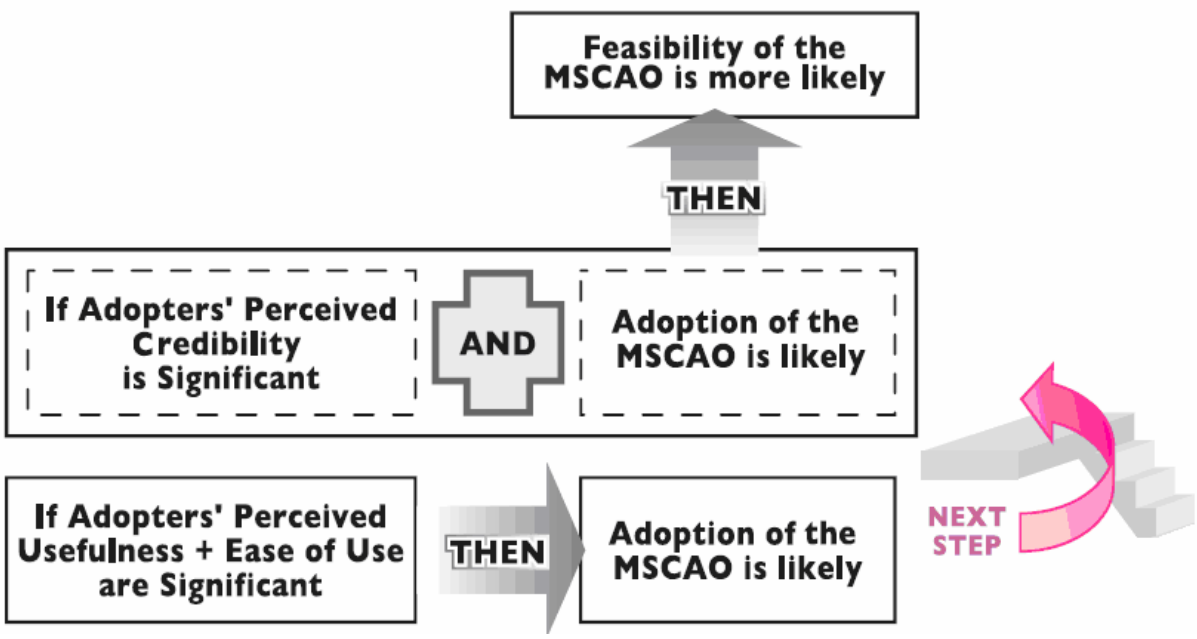


Figure 4: Primary hypothesis illustrated

Hypothesis 1 (H_1)**:** *"Perceived Usefulness" and "Perceived Ease-of-use" are positively correlated to likely adoption of the MSCAO;*

Hypothesis 2 (H_2)**:** *"Perceived Usefulness" is positively correlated to "Perceived Credibility" with regards to the likely adoption of the MSCAO;*

Hypothesis 3 (H_3)**:** *"Perceived Usefulness" is more important than "Perceived Ease-of-Use" when considering the likely adoption of the MSCAO;*

Hypothesis 4 (H_4)**:** *"Perceived Credibility" is more important than "Perceive Ease-of-Use" when considering the likely adoption of the MSCAO;*

Hypothesis 5 (H_5)**:** *Electrical engineering students display a more positive attitude toward the credibility of the MSCAO than electronic engineering students.*

CHAPTER SUMMARY

The foregoing discussions covered previous research relevant to this dissertation. The documents reviewed included various academic publications, patent searches, and declassified military reports. In particular, the researcher discussed key concepts and theories associated with users' adoption of emergent technologies. He established the relevance of previous literature covering airborne

symmetrical interaction between the system and the user. The literature also revealed several existing user models (Maes, 1994; Lau, 1997; Farrell, 2000; Brown, 1998; Bomsdorf, 1996).

EMPLOYMENT OF SCENARIO PLANNING JUSTIFIED

As the literature review suggests, *scenario planning* is a strategic planning technique used to make flexible long-term plans (Armstrong, 1978; Ringland, 1998; van der Heijden, 2002; Schwartz, 1991). In the context of a 21st century dynamic information-driven society, "scenarios" are gaining credibility as effective tools to prepare for an uncertain future, test decisions, alter mental models, and improve performance (Chermack *et al.*, 2001). In fact, Chermack and Lynham (2002) presented a complete review of definitions, paradigms, and a capacious historical background of scenario planning. A snapshot is offered below:

> Scenario planning first emerged for application to businesses in a company set up for researching new forms of weapons technology in the RAND Corporation. In 1967, Herman Kahn of RAND Corporation pioneered a technique called 'future-now' thinking. The intent of this approach was to combine detailed analyses with imagination and produce reports as though people might write them in the future. Kahn adopted the name 'scenario' when Hollywood determined the term outdated and to the label 'screenplay.' In the mid-1960s, Kahn founded the Hudson Institute, which specialized in writing stories about the future to help people consider the 'unthinkable.' He gained most notoriety around the idea that the best way to prevent nuclear war was to examine the possible consequences (p. 367).

In this respect, *scenario planning* is closely related to foresight methods (e.g., Bayesian models, game theory, pattern matching, Delphi, and econometrics) frequently used by military planners. Nonetheless, *scenario planning* is not restricted to military intelligence. For instance, Ahlqvist (2005) used Delphi techniques to identify key information technologies associated with various dynamic sectors (such as academic and corporate settings).

In sum, scenario planning assisted the researcher in making key decisions about the evolution of the cyber-WMD threat (including the exploration of the respondents' perceptions regarding the proposed MSCAO). It is through the same

line of reasoning that the researcher sought to find the potential solutions. The seven cases listed below were presented to the respondents during a pre-survey session:

Case-1: This computer animation depicts three apples being scanned by a biosensor to extract aromatic information (digital encoding phase). Once the olfactory information is digitized, a network protocol (TCP/IP)[4] transports the digital information over the Internet. At the receiving end, the animation shows a decoding process, a hand shake between the digital code and an on-board fragrance grid (APPENDIX I). When a match is made between the code and a specific capsule, the content of such capsule is chemically activated to release an aroma. Energy sources may include ultrasound, ultraviolet light, or laser.

Case-2: This is another still picture illustrating the application of the *MSCAO* in the decontamination of an aroma-embedded information system. This system was originally setup to allow computer users to share olfactory information (Figures 14 & 15).

Case-3: This still picture illustrates the application of the *MSCAO* in digital printing devices (printers, faxes, portable photo labs, copiers, and others): A warfare agent is detected, the Microfluidics process of the printing device is suspended and a warning system is activated. An optional diffuser may release an antibody to mitigate the harmful effects of escaped airborne contaminants (APPENDIX I).

Case-4: Another segment of the computer animation (the neutralizer) shows a module of detection that is capable of scanning for airborne molecules and finding a counter-agent from on-board chemical precursors to neutralize the detected threat. The animation also shows a mixing process of different chemical precursors to formulate a decontaminant at the potency dictated by a neural network that handles chemical requests. Once the precursors reach their final mixing stage, a pump is automatically activated to disperse the decontaminant in the infected environment (APPENDIX I).

Case-5: This segment shows the automatic dispersion of a polymeric antibody inside of an airplane (APPENDIX I), upon the detection of an unwanted substance. This case illustrates a possible extension of the *MSCAO.*

Case-6: This is a still picture illustrating the application of the *MSCAO* in the protection of public water systems. A deadly bacterium is detected; the water flow

[4] TCP/IP is acronym for Transmission Control Protocols/Internet Protocols.

(via faucets or distribution valves) is automatically suspended and a warning system is activated (APPENDIX I).

Case-7: Yet another segment illustrates the binding process of aerosolized decontaminants with airborne warfare agents to create a gravity-based precipitation of the free molecules (Valentine *et al*., 2004). First, biophysical properties of the molecules allow a collision that is used to form a cluster. Second, even with the influence of the Brownian law (Einstein, 1926) on particles in motion, several clusters are still maintained by the polymeric nature of the proposed decontaminant (APPENDIX I).

Summing up, the seven cases above covered the representation of (a) standard autonomous biochemical decontaminator (ABCD) and (b) LoC embodiment of the same system.

Standard Autonomous Biochemical Decontamination System

As shown in Figure 7 (below), an Artificial Intelligence module (8) will process digital information received from the detection component in order to formulate a neutralizing substance *in situ*. The AI module will be supported by a neural network to match chemical decontaminants against poisonous agents. Once the right "neutralizer" is formulated from on-board chemical precursors (5), displacement of the final product may be triggered by pressure valves (4) [which are attached to a plurality of containers (3) and connected to the mixing chamber (2)], to move the neutralizer from the mixing chamber to the diffuser (1). A rotating spindle (6) facilitates the permutation of the containers. Under pressure (7), the velocity and volatility of the concentrated formula augment to facilitate the dispersion of the final neutralizing substance. Telecommunication and warning systems embedded within the detection module (8) will alert authorities and advise potential victims. Below is a functional summary of the major components/modules.

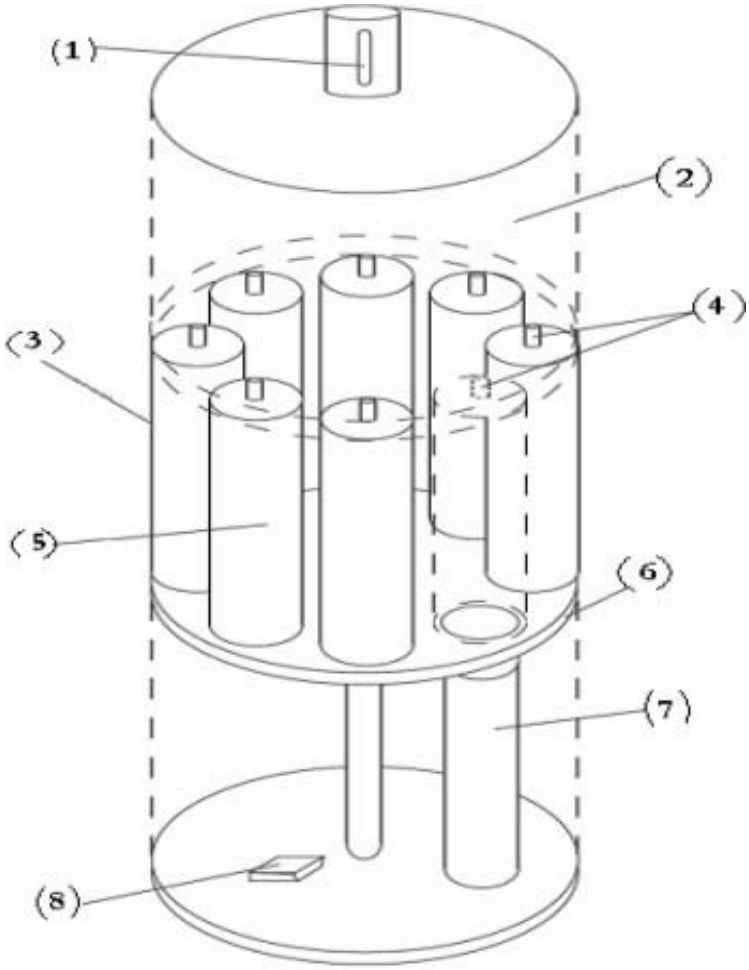


Figure 7: Schematics for the standard embodiment of the ABCD

Lab-on-Chips Embodiment of the *MSCAO*

In Figure 8A, a system-on-chip (SoC) embodiment of the proposed apparatus may allow a safer environment for the emerging cyber-assisted olfactory information exchange phenomenon and morph cell phones into ubiquitous sensors/decontaminators. The olfactory intake is scanned by a biosensor that assigns a digital fragrance code, which is used to locate a specific chemical (Figure 8C) from a chemical bank. The final release passes through a cyber-WMD screening (Figure 8B) before exiting the exhaust to the end user. Zhang et al. (2002) offer an interesting primer on the design and simulation of microelectrofluidic systems.

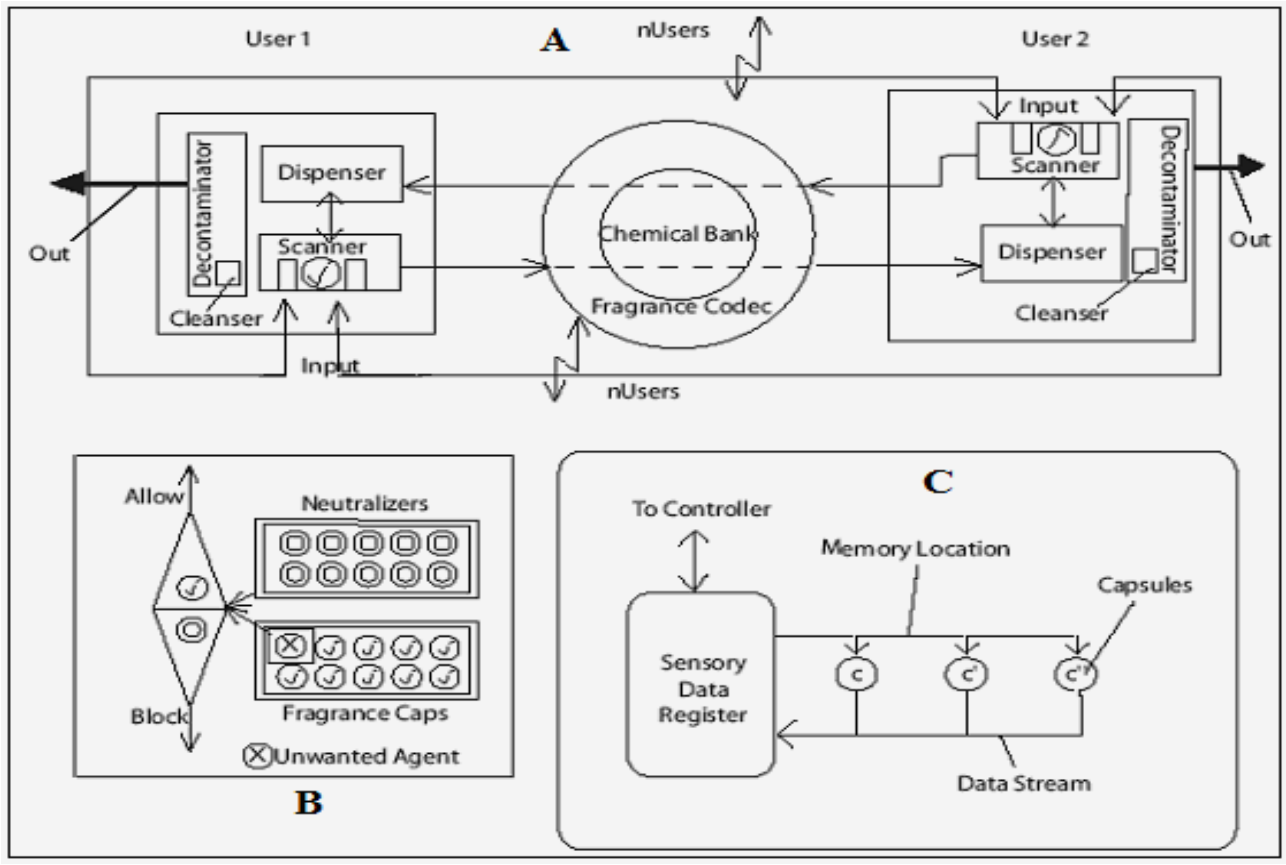


Figure 8(A, B, & C): Model for safer cyber-assisted olfaction (Hyacinthe, 2006b)

Detection module

In the context of an aerosol-based decontamination mechanism, it is logical for concerned critics to cast skepticism over the ability of the proposed apparatus to simultaneously determine the position, momentum, and properties of an airborne chemical. However, in response to the so-called Heisenberg[5] challenge, the researcher proposed the use of remote and mobile peripheral devices or miniature robots/ UAVs (with scanning and "beaming" capabilities) to facilitate the tasks of locating and mapping the trajectory of a chemical plume or measuring and recording "near-perfect" positions of an airborne chemical's point of release. Essentially, the detection component comprises a plurality of multi-array sensors of various types connected to a sensory data fusion module (SDFM). The SDFM allows the parallel processing of multi-source heterogeneous data from these sensors through a neural network. Among other techniques, surface Brillouin scattering (SBS) [6] can be

[5] Heisenberg, W. (1927). Ueber den anschaulichen Inhalt der quantentheoretischen Kinematik and Mechanik. *Zeitschrift für Physik 43*,172-198. English translation in (Wheeler and Zurek, 1983).

[6] Beghi, M., Every, A., and Zinin, P. (2003). *Engineering and Biological Material Characterization* [Chapter 10, pp. 581-651]. Boca Raton, Florida, CRC Press.

exploited to measure other properties, like the layer thicknesses or mass density, or the presence of interfacial layers.

Neural network AI module

The neural network serves as an interface between the detection module and the storage facility. In essence, it connects sensory data from the detection sensors to a plurality of chemical precursors through various pattern matching techniques (graph theory, matrix manipulation, and clustering).

Storage (Neutralizers) module

The storage facility holds a series of important chemical precursors (primarily neutralizers and decontaminants) that can be mixed in proportion and concentration as directed by the AI module. These precursors are contained in a plurality of small capsules or in large tanks (depending on the setting). The inventory of the chemical precursors is kept by an electronic metering system that allows the tracking of the quantity dispersed from each container at any time.

Mixing chamber

This chamber mixes precursors as directed by digital logics of the AI module. The neural network synchronizes the activities between various modules. Thus, this mixing chamber serves (among other duties) as a portable chemical laboratory (Le Gac *et al*., 2001; Le Gac *et al*., 2002; Le Gac *et al*., 2003) that prepares on-board chemical precursors for final release.

Binary delivery aerosol system

The final release may be premixed or mixed *in situ*. When the latter approach is used, the system is said to be operated under a binary delivery system: an effective approach used in chemical weapon development to designate a weapon system that is deployed in stages. Thus, precursors can be stored at various chemical states (solid, liquid, or vaporous). Although applied pressure will yield a certain quantity of vapor, the final release may be in the form of granular or hydrate droplets. For example, the volume of aerosol as well as its tissue factor (TF) against undesirable agents can be monitored through procedures based on luminol and peroxyoxalate reactions. Other emerging biosensor technologies may render such task even less wearisome.

Other Applications/Auxiliary Systems

As shown in Figure 9 below, the autonomous biochemical decontaminator can be embedded in subway systems (71) as well as in cruise ships (72). In addition, it can be installed in airports and aircrafts (73), as well as in churches and sport arenas (74). These sites have been designated as potential terrorist targets by most intelligence agencies.

Metaphorically, as water sprinkler systems allow or suspend water flow through a pipe, a cost-effective embodiment of this apparatus (APPENDIX-F) may work in similar fashion for an entire community, in the event of a biochemical attack on the public water supply. Baeumner *et al.* (2001) already developed a detection module (a biosensor) inline with the principles being discussed here. Their biosensor detects *C. parvum* messenger RNA (mRNA) molecules, which are only present in organisms that are alive. Their research effort was supported by the Bioanalytical Research Group, Department of Food Science and Technology at Cornell University, USA (p. 1176).

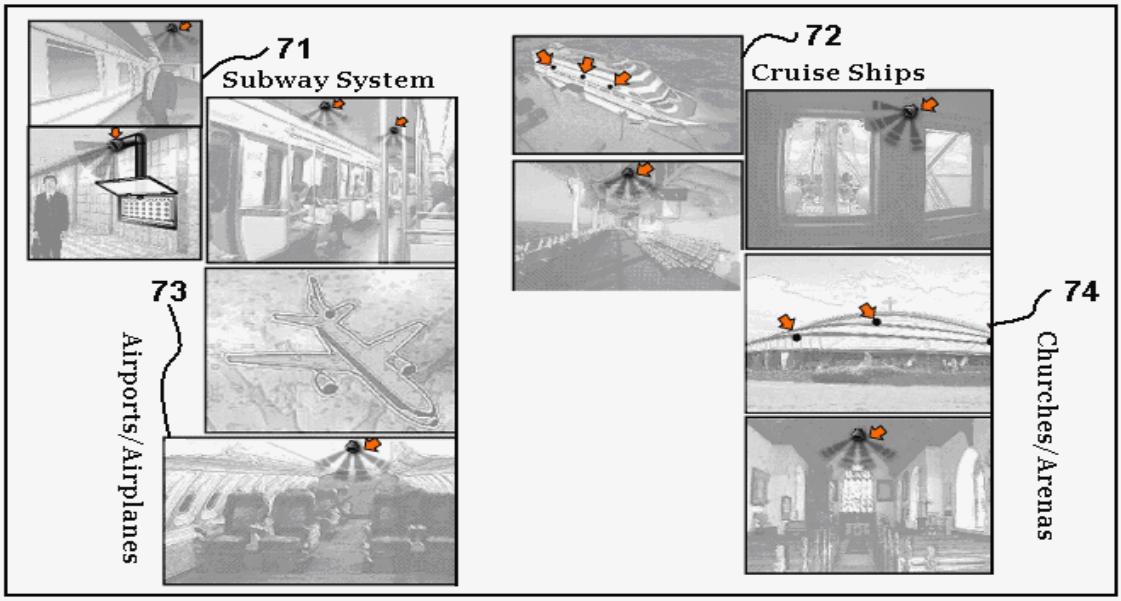


Figure 9: Applications in aviation, mass transit, and dwellings

Through this disssertation, a more advanced system that can be placed as a biohazard “stopper” at the terminus of tap water lines in residential and industrial installations is proposed -not just another detect-to-warn system (APPENDIX-F).

In effect, the proposed model encompasses standard systems and μTAS. It features an autonomous biochemical neutralization process that may be applied in a variety of settings to include entertainment, medicine, and defense and security. Further development of this concept may encourage pharmaceutical companies to

develop drugs that can be administered through inhalation, for the popularity of cyber-assisted olfaction will facilitate drug distribution through new channels and sites. For example, a group of individuals in need of medicine might not have access to medical personnel. In this case, a special embodiment of this apparatus could serve as a "robot" pharmacist or e-nurse.

Based on lessons learned from users' adoption of emergent technologies, the researcher concluded that both traditional intelligence agencies and unconventional paramilitary/terrorist groups will compete for the most effective weapons of the future. Consequently, under the paradigm *messianic singularity vs. lethal mutation* (Hyacinthe *et al.*, 2007), the researcher developed and sought patent protection for several innovative concepts discussed in the next section.

As illustrated in Figure 9, the ABCD is offered as a preemptive strike[1] against a serious threat to mass transit, aviation, and cyber infrastructures. A three-step illustration of the original concept is provided below (see Figure 10). The detection step involves "*capturing"* sensory data via a network of heterogeneous biosensors. The "*computing/neural networking*" step involves localized and remote processing by avatars and intelligent agents via Web services, which link the first step to the third. The "*neutralizing/decontamination*" step ensure optimal execution of requests to mitigate detected biochemical threats (such airborne) via a network prioritization delivery service at the middleware level of the proposed system. The ABCD carries several added values. For example, a hand-held embodiment of this device may consist of a compact tank (such as a multi-compartmental cylinder loaded with various decontaminants) surmounted by a set of multi-array biochemical sensors. In the presence of a bioactive substance, human operators will be alerted to activate the device by releasing a neutralizing fluid in the air to provoke an aerosol-based environmental decontamination reaction (Figure 10). In the future, this hand-held embodiment can be mass-produced at a more reasonable cost than the fully-autonomous system, which is intended to work in much larger settings. Moreover, for the protection of public water distribution systems, the apparatus may be programmed to detect a bio-threat, shutoff water pressure valves, send warning signals to authorities, and release a cleansing fluid to mitigate the offending agent's expected harmful effects (APPENDIX 13).

[1] Malcolm, D. (2001). Genomics and Future Biological Weapons: The Need for Preventative Action by the Biomedical Community. *Nature Genetics, 29*, 253-265.

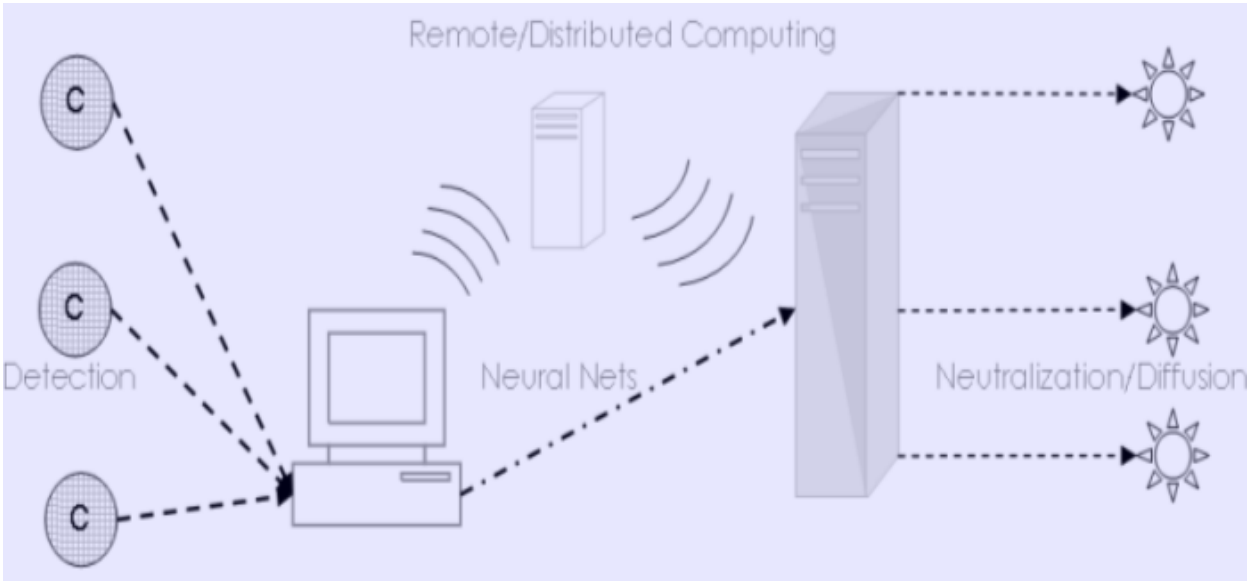


Figure 10: 1-2-3 of the ABCD

DESIGN OF THE STUDY

Survey Instrument

Although survey has been rated as the most popular method of data collection and analysis, designing and administering a survey is not a simple and straightforward matter (Groves, 1989). It requires careful planning and in-dept knowledge of existing survey protocols. Nonetheless, among many advantages, surveys provide a means to collect quantitative data. Because of their orientation towards quantitative studies, social scientists have used the survey method extensively and gained very useful insights in the process (Rosnow and Rosenthal, 1996; Salant and Dillman, 1994).

Since there are literally thousands of survey professionals and social scientists conducting surveys and publishing their results on every conceivable topic, it is reasonable for a researcher to use a set of constructs that have been used and tested by established investigators, when the instrument is calibrated under similar theoretical principles. Although alternative social science methodologies are available (McKenna, 1995; Frankfort-Nachmias and Nachmias, 1996), the survey method remains a very reliable source of primary data collection. Secondary data sources (i.e., third party dataset and previously used dataset) might have a certain advantage (such as time-saving) but the lack of control over what information was collected and how it was collected (Frankfort-Nachmias and Nachmias, 1996) makes it less desirable. Based on the foregoing considerations, a survey questionnaire was prepared and administered as soon as the human subject clearance was granted.

Essentially, the researcher used the survey instrument to explain causality between perceived credibility, perceived usefulness, and perceived ease-of-use. In fact, according to Bryman (1984), survey methodology is suitable for explaining causality between observed variables and latent variables and testing hypotheses and established theories. Notwithstanding certain disadvantages, surveys offer (1) substantial external validity (Cook and Campbell, 1979), (2) tremendous support for describing the characteristics of large samples (Salant and Dillman, 1994; Henry, 1990), and (3) great opportunities for reusability (Babbie, 2001). Although the advantages often overweigh disadvantages, surveys are also known to be too inflexible, somewhat too artificial, and in some cases too weak to capture erroneous responses. To overcome these challenges, the researcher was very methodical in selecting relevant constructs, establishing reasonable scales, and making post-pilot generated adjustments.

Informal Interviews

Complementary to the survey instrument, the researcher originally intended to collect in-depth responses from the respondents to "enlighten or provide clues that are followed up within the core method" (Morse, 2003, p. 190). However, based on certain constraints (covered in the enumeration of limitations of the study), tacit knowledge generated from informal interviews with a group of experts served as a viable option. Based on the preliminary results of the survey instrument, the researcher concluded that the anticipated follow-up interview was not a necessary condition to perform the level of analysis necessary to formulate an informed opinion on users' adoption of emergent digital information technologies. In fact, the comparative content analysis coupled with informal interviews of several experts familiar with the topic proved to be very useful in this case. As for the representation of the model, basic spatial mechanisms are discussed in the next section.

Representation of Cognitively Complex Concepts

Information science research is an area where there is some degree of cohesion around models and methods that have won some support (i.e., Shannon and Weaver, 1949; Buckland, 1991; Wilson, 1981, 1984, & 1999; Kuhlthau, 1991). However, teaching cognitively complex concepts (Heinrich *et al.*, 2001) might require a different set of tools. With more emphasis on information technologies, nonetheless, social scientists seem

to have developed a new consensus[8] towards the use of more dynamic models to support their arguments.

For instance, Ostrom (1998) noted the use of computer simulation as an alternative to the familiar verbal argumentation and mathematical models. In addition, the literature reveals that models are used in a variety of disciplines to represent knowledge and develop new theoretical frameworks (Weiss, 1979; Hanney 2002; Mead *et al.*, 1991; Lavis *et al.*, 2003).

Many social science inquiries have been built on simplified representations of social phenomena. These representations are often purely literal. However, the difficulty with such "verbal" or "sentential" presentations is evident in the struggle met by researchers and readers alike in deciphering cryptic information inherent to any emerging technology. With the evolving trends of digital technology-oriented social science research, more innovative techniques are being explored.

Block-diagrams and dataflow charts are basic spatial mechanisms often used to visually represent complex bodies of knowledge and explain sophisticated concepts to the external world (Markus, 1987; Coyne, 2002). According to Hunt (1991), diagrams and sketches are used to keep track of reasoning during 'decompositional' problem solving: complex problems are broken down into parts that can be treated easily enough, and partial results are integrated later on. In the engineering field, for instance, block-diagrams are used to represent very complex processes and systems. As a result, the researcher adopted a diagrammatic approach of representing knowledge relevant to the proposed *MSCAO*.

Use of Models to Foster Understanding

Models are commonly used to create understanding of emergent digital information technologies. For instance, Mukherjee and Fedder (1998) provided several recommendations pertaining to the design of systems-on-a-chip. Along the same lines, Chatterjee and Aluru (2005) proposed a model and simulation of integrated circuits. Moreover, several computer programs or software are also available to simulate microfludics processes and LoC activities. For example, CoventorWare[9] features microfluidic behavioral models to allow top-down system-level design. Although a majority of Microfluidics systems in use today are droplet-

[8] Consensus here is used to indicate a higher level of acceptance of digital information technologies and more dynamic IS models to represent complex knowlege.
[9] ConverWareTM. Available: http://www.conventor.com

based systems, it is important to note that LoC is not limited to liquid droplets; other chemical states (gaseous in particular) can be detected, processed, and analyzed in similar fashion. Hence, the researcher utilized a model to explore some mechanisms, principles, and apparati that may be available against the identified threats to emerging cyber-assisted olfaction technologies.

Hybrid Methodological Approach

Although quantitative research is equally (individually) important as qualitative research, several scholars have suggested the triangulation process of combining two or more research methods in order to offer a more complete picture of their academic investigations. Detailed discussions of triangulation are held in (Mingers and Gill, 2001). Notably, Markus' (1987) paper on electronic mail illustrates the application of triangulation in empirical research.

Accordingly, the adopted hybrid methodological approach involved the comparative content analysis of several data streams (patent search, declassified military reports, expert testimonies, survey, and interviews). The researcher selected ANOVA and other statistical analysis techniques to analyze (across various data sources) the feasibility, *credibility*, usefulness, and ease-of-use of an emerging technology. For example, the MANOVA technique tests one group or several groups to determine if there are differences on two or more variables. As the results of this study suggest, statistical analysis of variances can be used in combination with qualitative approaches to strengthen data analysis and interpretation (see Cohen, 1988).

METHODOLOGY JUSTIFIED

A careful review of the literature revealed an evolutionary movement to customize traditional grounded approaches into more expandable, practical research tools. For instance, Charmaz' (2000) constructivist approach to grounded theory, Strübing's (1998) simulated grounded theory, and Soulliere, Britt, and Maines' (2001) grounded conceptual modeling are listed among several other tools. In addition, Yoong and Pauleen (2004) described how they used a grounded action learning approach (a synthesis of grounded theory and action learning methods) to produce a flexible methodology, which is feasible to conduct applied research of emerging technologies. As the literature review revealed, statistical analysis of variance is widely used in social science research, notably in behavioral and socio-technological

inquiries. An elaborate discussion of this statistical tool is found in (Harris, 1993; Dekker and Olson, 1996).

Of interest, in this section at least, is the mixed-methods analysis approach that includes qualitative and quantitative methods to offer a comprehensive framework for safer cyber-assisted olfactory information exchanges in standard and micro systems. Finding the right method to evaluate an emerging technology is a challenge that necessitates careful considerations of a user perception-based model. A *hybrid method* approach consisting of Rogers' IDT and Davis' TAM further extended these two theories (Venkatesh and Davis, 2000) to create a more fertile environment for data collection and analysis. Since an entirely separate chapter is devoted to data collection and analysis (see Chapter 4), only an introductory discussion is held on data collection, data quality, impartiality, reliability, and avoidance of bias in this chapter.

Data Collection

Data was collected from various sources via a variety of collection techniques. For instance, the literature served as a preliminary data collection technique (details on the literature review are provided in Chapter 2). The researcher also collected data from patent searches and a series of declassified military reports [10] (further elaboration is provided in Chapter 5 covering data analysis). Last, but more importantly, a survey instrument was designed to collect data from a group of seventy (70) engineering students.

Survey instruments must go through a rigorous process to avoid common mistakes, which may discredit any study built on such instruments. To avoid chronic mistakes, pilot testing is often used as a golden rule in designing a questionnaire. Thus, as recommended in (Babbie, 2001), upon receiving feedback from the pretest group and the dissertation committee, the researcher reworded confusing questions, reorganized the questionnaire, removed unnecessary questions, and finally administered the survey instrument.

Data Quality

Qualitative research produces large amounts of textual data in the form of transcripts and observational field notes (Glasser and Strauss, 1967). The systematic task of preparing and analyzing these data is time consuming and labor intensive.

[10] Declassified reports (e.g., ADA388953; ADA407502; ADA236609; ADA346005; ADA407098) from Naval Post Graduate School. http://library.nps.navy.mil/home/bibs/chemtech.htm.

Data analysis often takes place alongside data collection to allow questions to be refined and new avenues of inquiry to develop (Dey, 1993). Thus, in order to provide high quality of data collection and to ensure impartiality, the researcher identified and examined all the data relevant to each step of each technique through a process of continuous comparative analyses. In addition, each item was checked or compared with the rest of the data to establish analytical categories. As a result, a coherent and systematic approach was put in place.

Reliability and Impartiality

The researcher also made the decision to use grounded theory principles which, via sequential analysis or interim analysis, allowed him to go back and refine questions, develop hypotheses, and make necessary adjustments that further support data integrity (Becker, 1971; Miles and Huberman, 1984; Glasser and Strauss, 1967). Textual data are typically explored inductively using content analysis to generate categories and explanations, the acquisition of high quality data depends on the researcher's skills, vision, and commitment.

Avoidance of Biases

With respect to impartiality and high quality data, the researcher used measures (e.g., how to capture all reported data exactly as received) intended to provide logical consistency among all parts of a record, to ensure that manipulation or transformation of the data produced no unintended changes, and to verify that statistical and arithmetic calculations were performed as planned. In addition, pilot testing and peer review were applied to ensure that information of appropriate depth, breadth, and specificity was collected and remained consistent over time. Carefully adapted instruments (such as TAM) assisted the researcher in making sure that acceptable levels of such attributes as validity, reliability, reproducibility, sensitivity and specificity were achieved.

ESTABLISHMENT OF CONSTRUCTS

Prior studies revealed several serious attempts to explain user acceptance (Swanson, 1974; Schultz and Slevin, 1975; Ginzberg, 1981). Although numerous individual, organizational, and technical variables have been investigated (Robey and Farrow, 1982; Benbasat and Dexter, 1986; Markus and Bjorn-Anderson, 1987), research has been constrained by the shortage of high quality measures for key determinants of user acceptance (Davis, 1989). The literature also indicated that

many of these measures do not correlate highly with system use (Schewe, 1976; Ginzberg, 1981), and this lack of standards tends to negatively affect research findings. The utilization of improved measures for key theoretical constructs is critical to foster understanding. Nonetheless, users' unwillingness to accept and use available systems (Bowen, 1986) may hinder the implementation of new technologies.

Therefore, in order to elicit perceptive responses regarding emerging aroma-embedded information technologies, the researcher presented a series of animated clips illustrating the activities of the major components of the proposed system. In order to select the most effective and scalable constructs, the researcher adopted the principles found in (Davis, 1989; Rogers, 1976) and reconciled them with Rogers' (1995) five innovation attributes (relative advantage, compatibility, complexity, trialability, and observability).

Observable Variables

Along with a diagrammatic illustration of their integration within the research design, the constructs, carefully selected for this questionnaire, are presented, defined, and explained below within the context of a broad definition of technology adoption. Information technology adoption is the decision to accept, or commit to a particular technology (Rogers, 1995; Venkatesh and Davis, 2000). Note that the terms adoption, use, and acceptance are used interchangeably across many disciplines to discuss users' positive responses toward a new technology.

According to McFarland and Hamilton (2006), the technology acceptance model of Davis (1989) is strongly connected with Rogers' model. The technology acceptance model purports that the individual's intention to use is the "single best predictor of actual system usage" (Davis and Venkatesh, 1996, p. 20). As cited above, the technology acceptance model has been used extensively to anticipate, explain, and understand users' adoption of new technologies. Acceptability was adopted from its meaning established in (Luarn and Lin, 2005). They effectively used similar methods to determine their subjects' perceived usefulness and perceived ease-of-use of a computer system. According to their findings, individuals accepted a computer technology if they are willing to use it.

Latent Variable

Latent variables are widespread in the social sciences. Whether it is intelligence or socioeconomic status, many variables cannot be directly measured. Latent variables are variables that are not directly observed but are rather inferred from other variables that are observed and directly measured. In this study, adoptability is considered as the latent variable. Examples of latent variables include business confidence, morale, and intentions, which may be very challenging to measure directly. However, given a technology model linking the latent variable to other observable variables (such as usefulness, ease-of-use, and credibility), the values of the latent variable (adoptability) can be inferred from measurements of the observable variables.

One advantage of using latent variables is that it reduces the dimensionality of data. A large number of observable variables can be aggregated in a model to represent an underlying concept, making it easier for humans to understand the data. As such, the observable variables (usefulness, ease-of-use, and credibility) were assembled according to the TAM and IDT to represent the MSCAO. At the same time, the latent variable (adoptability) links these symbolic, theoretical constructs (credibility, ease-of-use, and usefulness) to the real users' intent to adopt emergent technolgies. Factor analysis then incorporates the latent variable during hypothesis testing. Factor analysis is a statistical data reduction technique used to explain variability among observed random variables in terms of fewer unobserved random variables called factors.

Perceived Adoptability

The degree of adoptability of a model indicates how likely the resulting system is to be accepted. As such, adoptability is a latent variable, which is inferred from scores obtained for the observable variables. In other words, it can be considered as a predictor of how likely the resulting product is to move from model to fabrication. In this study, it is argued that students' unwillingness to accept and use an emerging technology can be considered as a (negative) feasibility factor. It is further argued that students' unwillingness may be associated with a rejection of the model utilized to represent the technology being examined. *Perceived adoptability* is established in this study as a *dependent variable* on usefulness, ease-of-use, and credibility (*the observable variables*). Perceived adoptability is measured by the perceived

practicality (usefulness and ease-of-use) and the perceived trust (credibility and security) of the proposed system (Figure11).

Perceived Usefulness

Usefulness is an observable variable that measures the purposefulness of the system as it relates to solving a problem, satisfying a need, or addressing a threat. Bandura's (1986) self-efficacy theory provides a theoretical perspective, establishing a very interesting relationship between perceived ease-of-use and perceived usefulness: they function as basic determinants of user behavior. According to Bandura, in any given instance, behavior would be best predicted by considering both self-efficacy and outcome (p. 140). The researcher adopted a definition for this construct, which is consistent with propositions found in (Venkatesh, 2000; Dishaw and Strong, 1999).

Perceived Ease-of-Use

This observable variable measures the degree of difficulty of the system. It encompasses ease of access to devices and ease of manipulation of various features. Effortless, ergonomic, flexible are attributes also associated with this construct. Davis (1989) defined ease-of-use as "the degree to which a person believes that using a particular system would be free of effort." Notably, Karahanna and Straub (1998) provided similar definitions.

Perceived Credibility

The word credible can be traced to its Latin root *credere*, to believe. Fogg (2003) found that believability is a good synonym for credibility in virtually all cases (p. 122). In this study, "perceived credibility" refers to the respondents' observed trustworthiness and capabilities of the proposed *MSCAO*. Essentially, credibility is an observable variable that measures the degree of tolerability of the system. In the current context, it is hypothesized that students are likely to accept a tolerable, credible technology over a disagreeable, unsafe one. Perceived credibility also measures how welcome the respondents find the system. In short, it translates 'how welcome' they perceive the proposed system.

As stated above, the researcher utilized constructs that have been previously tested and proven to be effective means of determining users' intention to adopt emergent technologies (Figure 5), based on the concept shown in in Figure 11.

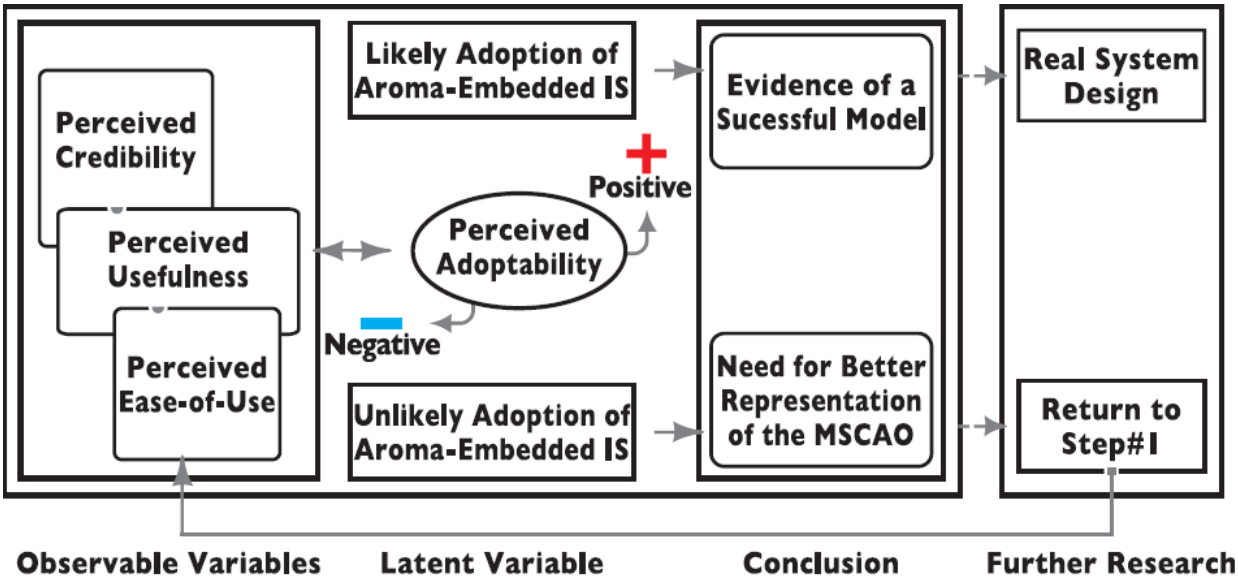


Figure 11: Original conception of the constructs

As illustrated in Figure 11, perceived credibility, perceived usefulness, and perceived ease-of-use constitute the observable variables, while perceived adoptability accounts for the latent variable. The researcher used the scores of the observable variables to determine their level of influence (high/low) on the latent variable (adoptability). As shown in Figure 11, the researcher hypothesized that a highly positive level of adoptability would imply the likely adoption of aroma-embedded information systems and a very low level of adoptability would imply an unlikely adoption of aroma-embedded information systems. The researcher also provided a feedback loop that would allow changes to be made to model until an effective representation obtained. As suggested in Figure 11, the passage from model to prototype to system fabrication would only occur after the realization of a successful and feasible model.

RESEARCH PROTOCOLS EXPLAINED

Methods and Procedures

Questionnaires were administered over a three-week period to a convenience sample of 70 engineering students at a large southeastern university. Prior to selecting convenience sample, the researcher reviewed a variety of techniques and the mechanisms (Babbie, 2001; Salant and Dillman, 1994; Henry, 1990; Frankfort-Nachmias and Nachmias, 1996) to ensure that the selected technique is appropriate and compatible to his study.

With the permission of the instructors, the respondents (graduate and undergraduate college students) watched a series of PowerPoint slides and answered the twenty questions presented to them during class sessions. Participation in the survey was voluntary, and the responses were kept confidential.

The stimulus was a PowerPoint presentation related to cyber-olfaction technologies and emerging physical cyber security protocols. See Appendix I for the stimulus PowerPoint slides. In consultation with professional graphic artists and several electrical engineers, the researcher designed the audio-video components as stimuli.

A narrative of the scenarios accompanied the video clips. The scenarios were illustrated in cases (see scenario planning in subsequent discussions). This was done to provide a realistic graphic user interface (Schneiderman, 1997) for participants to view.

The respondents watched the fifteen-minute PowerPoint presentation and spent another twenty minutes to answer the survey questions. An independent proctor collected data and forwarded the consent forms and survey responses to the researcher. The data were analyzed using SPSS 15.1. Responses were manually entered. Data entry was verified by visually checking each survey against the data file to ensure all entries were correct. Results of the analysis are presented in Chapter 4.

However, there are several limitations to these procedures. First, the researcher used convenient sample of college students. Second, generalization and extrapolation will need to be done with appropriate supporting data. Third, the stimulus had to be carefully designed and applied to avoid a potential bias (e.g., the fear factor). In sum, the survey instrument was used in connection with a comparative analysis of a series of patent searches and military reports, in order to reflect the multidisciplinary nature of this dissertation and to present a holistic picture of the researcher's envisioned *flexible framework* for better understanding of various aspects of cyber-assisted olfactory information systems. As such, this mixed-methods approach (Mingers and Gill, 1997) allowed the researcher to gather, obtain, and analyze data from various sources in order to overcome shortcomings inherent to the traditional single method approach.

Follow-up interviews were originally scheduled to answer questions -that might arise during data analysis- and to gather input and recommendations from the interviewees. However, since no major issues emerged from data collected and several

experts were available to comment on the model, the researcher opted to conduct informal interviews with national security experts, e-noses experts, biochemists, and physicists who provided useful insights regarding the design, feasibility, and potential implementation of the proposed *MSCAO*.

Population of the Study

The study specifically focused on a group of college students' perceptions regarding the adoption of the theoretical model. The study sample consisted of undergraduate and graduate students enrolled in the Electronics Engineering program at the FAMU-FSU College of Engineering.

The survey was distributed to a sample of seventy (70) students enrolled in the program. As a condition of admission to the engineering program, all the students received the same basic educational preparation. Thus, the perception of the students surveyed is likely to be shared according to this common educational background. Therefore, respondents were selected regardless of their academic ranking (i.e., freshman, sophomore, junior, or senior). Population selection and sampling are discussed in details below.

In essence, the program of Electronic Engineering was selected for its pragmatic hands-on approach to electronics (in particular) and engineering (in general). While many engineering schools continue to focus on theoretical design and computer simulations, this hands-on approach makes the selected institution the ideal site to collect opinions on the "intent to adopt" the proposed model.

Questionnaire and Scales

The questionnaire provided a great opportunity to the researcher to collect useful information about a user's perception regarding intention to adopt emergent cyber-assisted olfaction technologies. However, in order to extrapolate and explicate the related findings, scalable constructs were indispensable. Accordingly, credibility, usefulness, and ease-of-use were selected and scaled. Consistent with the five-grade Likert scale, the researcher established five keys (1 = strongly disagree; 2 = disagree; 3 = neither; 4 = agree; 5= strongly agree).

Development of Scales

As shown below, during the development of these scales, the researcher assigned three main categories of questions, once the literature confirmed that these categories were proven and tested as relevant constructs to this study. The three categories corresponded to the three constructs (ease-of-use, usefulness, and usability). However, at the final stage, questions were randomly redistributed to facilitate the administration of the survey and to prevent systemic response bias (APPENDIX C). Pilot testing of the measures was done by employing a selective of respondents and experts. These individuals included Information professionals and defense and security experts who are familiar with protocols established. Each question encapsulates a descriptor that has been considered as representative or relevant to the construct. For example, the researcher used “easy” in one survey item in order to determine the degree of freedom to accomplish a specific task. The other tables contain similar information according to the construct considered.

As previously noted, the researcher used ANOVA to determinate validity and establish reliability. ANOVA was performed on the constructs and the results showed a larger F-ratio (69.9) and smaller p-value (.000), indicating a significantly smaller population standard deviation. Although the means of the constructs were different, there was not enough statistical evidence to deny their influence on users’ intent to adopt the *MSCAO* (Table 2).

Table 2: Three-factor ANOVA results (SPSS 15.0)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	46.326	1	46.326	69.864	.000(a)
	Residual	234.730	354	.663		
	Total	281.056	355			

a Predictors: (Constant), Credibility
b Dependent Variable: Usefulness

In sum, using Davis’ (1989) recommendations, pretest interviews were conducted to further enhance content validity by accessing correspondence between candidate items and the definition of variables they intended to measure (p. 324).

Pilot and Pretest

A survey instrument is a very delicate document. Even the most carefully designed survey can yield erroneous responses. Pilot and pretest provide an

opportunity to make necessary corrections. The validity of the instrument and the reliability of the responses generated depend heavily on these corrections. In this study, the validity of the instrument is by principles established by authoritative references (Venkatesh, 2000; Karahanna and Straub, 1998; Dishaw and Strong, 1999) on the subject.

Accordingly, in April 2005, a pilot study started with a series of database queries and concluded with feedback information from experts of several relevant disciplines. During that time, the constructs (later used in the final version of the survey instrument) were put to a pretest. Nine questions (three questions for each observable variable and one direct question about the latent variable) formed the basis for inquiring and interviewing during the pretest. Useful knowledge acquired from the pretest resulted into further literature review (Labaw, 1980; Martin and Bateson, 1986; Fowler, 1995; Strauss and Corbin 1990; Glasser and Strauss, 1967; Yin, 1984) on survey design. Another stream of literature was equally important as it related to innovation diffusion and user acceptance models (Davis, 1989; Rogers, 1995). Subsequent to the realization of the recommended measure of reliability and validity, the instrument was adjusted into its current version.

Mixed-Methods Approach to Data Analysis

During the pilot testing a large amount of qualitative data was collected and the survey instrument returned a large amount of more quantifiable data. Qualitative and quantitative data were consolidated with the post-interview data to offer a more holistic picture of the *MSCAO* and particularly to the students' intent to adopt aroma-embedded information systems.

As Yin (1984) suggests, interviews can be utilized to answer "why" and "how" questions and to complement surveys that normally deal with the "what" questions. Nevertheless, since the main weakness of qualitative instruments is connected to validity (Kaplan and Duchon, 1988), the interviews conducted with the national security experts allowed the researcher to gather feedback and acquire essential information to the overall analytical exercise. As mentioned earlier, surveys and interviews complemented each other to project a more holistic image. A tentative timeline was set to ensure timely review and completion.

Data Analysis and Interpretation of Results

A preliminary data analysis was conducted from the results of the patent search and the declassified military reports (APPENDIX E). At that time, Microsoft Excel 2000 was used to organize the data and simplify its representation. Lessons learned from this pilot project served greatly to the realization of the current version of the survey instrument. Further quantitative data analysis involved the use of SPSS. Principles of deductive logic and hypothesis testing were also applied for qualitative data analysis involving data triangulation/extrapolation. The researcher used regression analysis to explain causality between the constructs, while graphs and diagrams were used to illustrate these results. Given the fact that the researcher used a survey as primary data source, his strategy seems to be supported by Bryman (1984, p. 77) who stated that "…the problem of causality has been eased by the emergence of path analysis and related regression techniques to which surveys are well suited." In this dissertation, the construct *credibility* was regressed on *ease-of-use* and *usefulness*. The primary technique for testing the hypotheses in the study was Factor Analysis to test the pattern within the constructs. For scale assessment, a combination of confirmatory factor analysis and reliability analysis was used. Confirmatory factor analysis was used specifically to assess construct validity. Based on the results of the analysis performed, the researcher concluded that a system perceived as credible is more likely to be adopted.

CHAPTER SUMMARY

The primary research agenda was to offer a safer model for cyber-assisted olfactory information exchanges. As such, the researcher limited his presentation to a theoretical framework or *paper prototype*. For instance, a follow-up study may involve a computer simulation or working prototype -which may yield to an actual device. Nonetheless, it is worth noting that these self-imposed limitations are strategic choices that should not be considered as a burden on the quality of the dissertation. Descriptors were obtained by deconstructing validated instruments previously built on Davis' (1989) TAM to study users' adoption of information technology. For perceived credibility, Fogg's (2003) model for web credibility studies was used with additional input found in (Suh and Han, 2003; Vijayasarathy, 2004; Ramnath and Pavlou, 2002; Heijden *et al.*, 2003).

The researcher used the information collected from the experts to further analyze the data collected from the patent searches (APPENDIX D) and the military reports (APPENDIX E). Further, he made the connection between the student's statements, his original view, and the experts' pragmatic views.

In sum, this study is limited by the variables selected. As such, the validity of any conclusions regarding the influence of these variables on adoption of emergent technologies will have to be tested in future studies with controlled interventions. Simply put, the scope of extrapolation should be confined to selected variables, which were drawn from Rogers' IDT and Davis' TAM for the purpose of the current study. Further research should compare perceived feasibility of sentential representation with diagrammatic representation or before and after viewing the computer animations. Lastly, follow-up studies should explore students' friction about the use of aroma-embedded information systems.[1]

[1] According to Dr. Darrell Burke, anxiety is a very popular construct used in technology adoption research to determine friction of technology adopters.

CHAPTER IV: DATA ANALYSIS AND INTERPRETATION OF RESULTS

COMPARATIVE CONTENT ANALYSIS AND HYPOTHESIS VALIDATION

This chapter begins with the comparative data analysis between the patent search and the declassified military reports, which revealed a cyber-WMD threat associated with careless and/or terrorist adoption of emergent technologies. Once the survey was administered and the responses collected, the data analysis and interpretation followed according to protocols established in Chapter 1 and detailed in Chapter 3. The survey instrument was examined, using a t-test to determine whether or not the means of the variables tested could be assumed to be different (a difference in means would suggest different attitudes). To support the t-test, an F-test was conducted to verify statistical correlations among various components of the questionnaire (an insignificant difference in variances would suggest the existence of internal validity among such components). Specifically, this chapter covers the hypotheses drawn on the three variables (credibility, usefulness, and ease-of-use) in terms of their influence on the adoption of the proposed *MSCAO*. And at the end of the chapter the researcher provides a brief summary of relevance of the findings to his overall research agenda.

Based on the analysis performed, credibility, ease-of-use, and usefulness received scores significant enough to be considered as positively influencing potential users' adoption of the model. Though the results of the study were similar to several other technology adoption inquiries (Davis *et al.*, 1989; Keil *et al.*, 1995; Satzinger and Olfman, 1995; Taylor and Todd, 1995; Igbaria *et al.*, 1996), the *MSCAO* emerged as an original attempt to offer harm-reduction measures against an imminent biochemical threat to emerging aroma-embedded information systems. As the case is true for many endeavors of this type, the researcher formulated a set of hypotheses supported by a series of matching research questions in order to prepare the methodological landscape of his inquiry.

COMPARATIVE CONTENT ANALYSIS

Patent Search and Military Reports

Consistent with Weber's (1985) suggestions, the researcher performed a content analysis of forty declassified technical military reports, abstracts, and theses. The key themes used to query the military database were: biochemical weapons; weapons of mass destruction; emergency response; cyber security; use

of computers as weapons; future use of biological, chemical, nuclear, and radiological weapons; cyber terror; and Cyber-WMD nexus. The reports unanimously pointed to a looming threat associated with chemical, biological, nuclear, radioactive and high yield explosives on U.S. soil (Declassified Military Reports, 2005). The data retrieved raised even more disturbing issues, which called for further investigations. Accordingly, the researcher interviewed a group of national security experts to acquire tacit knowledge of the topic, a key factor to the overall data analysis.

The database of the U.S Patent and Trade Office (USPTO) provides very reliable information about emerging technologies. Although an issued patent does not guarantee acceptance, it is nevertheless, a good indicator of a proven theoretical framework for the possible realization of a device or apparatus. In June 2005, the researcher conducted a patent search with the assistance of a patent and intellectual property attorney (Christopher Paradies, PhD, JD) in the Tampa Bay area of Florida. As a result of this investigation, an evolving trend related to aroma-embedded information systems was noted (Paradies and Hyacinthe, 2005).

The United States Department of Defense (DoD) conducts most of its advanced research activities through DARPA. DARPA's database was also used as a preliminary data source through a review of on-going calls for research proposals related to the topic. DARPA is a vital source, for its calls for proposal go through a systematic process of consulting with leading experts (worldwide) on a particular topic or technology through a steering committee. The steering committee is usually tasked to avoid duplicates and to ensure that the actual proposal touches on new, revolutionary concepts. Secondary sources included the researcher's personal correspondences, academic literature, and relevant conferences and symposia.

A comparative analysis of data collected from the cited sources was performed with objectivity and impartiality and the lack of initiatives to counter the looming threats associated with certain aspects of these technologies particularly captured the researcher's attention. As such, the findings presented in Table 3 played an important role in the design and conceptualization of the proposed *MSCAO*.

In light of these reviews, the researcher launched a full investigation to explore perceived usefulness, ease-of-use, and credibility related to the proposed

MSCAO according to the perceptions of the respondents and through a carefully designed survey questionnaire.

Table 3: Snapshot of content analysis of patents and reports[12]

BIO-CHEMICAL THREATS /DECLASSIFIED MILITARY REPORTS AND THESES
ADA326609: *Terrorist Use of Weapons of Mass Destruction Within the United States: Asymmetric Warfare Paradigm in the 21st Century*. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, March 1997. [Lt. Col. M. Brown].
ADA407502: B*ugs & Drugs: Chemi-Bio Terrorism & the U.S. Government.* Quantico, VA: Marine Corps Combat Development Command, May 2002. [Lt. Col. W. Anderson].
ADA236609: *Responding to Chemical Attack.* Newport, RI: Naval War College, Department of Operations, February 1991. [Lt. Col. R.W. Bagley].
ADA346005: *New Enemy: Silent, Lethal, and Invisible*. Carlisle Barracks, PA: Army War College, April 1998. [Lt. Col. W.T. Bester].
…
ADA407098: *Role of the National Guard in Responding to Weapons of Mass Destruction (WMD) Attacks in the U.S.: Where Do We Stand.* Maxwell Air Force Base, AL: Air University, Air Command and Staff College, April 2001. [Lt. Col. M. Besosa].
ADA365438: *High Resolution Modeling of a Terrorist Chemical Attack in an Urban Area*. Monterey, CA: Naval Postgraduate School, June 1999. [Lt. Col. J. Broadwater].
EMERGING CYBER-OLFACTION TECHNOLOGIES/PATENT SEARCH
US5949522A: *A device is described which can deliver various combinations of scents in rapid succession in a user's nose* in conjunction with videographic images and/or sounds [Manne, J. (1999)].
US6524537: This patent disclosed a fragrance emitter used with internet. According to the inventor, *the fragrance emitter is able to emit various kinds of fragrance stored in vessels according to the command sent by a frequency detector* which is used to search for the existence of a specific frequency specially used by a specific website [Lee, C. (2003)].
US6004516: The inventors proposed an *apparatus for generating odor upon electronic signal demand using a disk having an aroma-impregnated adsorbent and a substrate* [Rasouli *et al*. (1999)].
…
US2004024043*: The inventors described an *information processing apparatus with an interactive scent interface to enrich users' perceptive experiences*. It is important to note that Wang and his associates even proposed a cell phone embodiment of their aroma-embedded information system [Wang *et al*. (2004)].
… Full abstracts related to these documents are provided in appendices D (patents) and E (declassified military reports). **** This is a publication number.***

According to the findings illustrated on Table 3, U.S. military scholars, from the Army War College (e.g., ADA326609), the Naval War College (e.g., ADA236609), the Air University (e.g., ADA407098), the Naval Post Graduate School (e.g., ADA365438), and the U.S. Marine Corps (e.g., ADA407502), have manifested great

[12] Partially inserted in the conference paper presented at the U.S. Naval Post Graduate School in Monterey, California on March 8, 2007 (See Hyacinthe and Anglade, 2007).

concerns over the imminence of a biochemical attack on U.S soil. Unfortunately, *cyber-olfaction technologies are being developed without capabilities that would reduce the dreadful effects of a potential biochemical attack involving today's ubiquitous digital gadgets*. It curiously appears that neither the reports nor the inventions warned against this potential cyber-WMD, a critical part of this research's concerns (APPENDICES D&E).

In addition, as illustrated in Table 3, the reports warned of "an intent to attack with" biochemical weapons and document on-going "attempts to acquire" such weapons. The patent search provided evidence of a significant number of inventors continuously and meticulously seeking to integrate olfaction as an innovative component of multimodal human-computer interactions, setting up the stage for scented emails, aroma-embedded Internet browsers, and cyber-assisted aroma therapy (Lee 2003; Manne 1999; Rasouli *et al*., 1999; Wang *et al*., 2004). More disturbingly, the patent search also revealed the introduction of this threat into the bedroom via aroma-embedded cell phones and other portable electronic devices (Wang 2004; Paradies and Hyacinthe 2005; Hyacinthe 2006a). The line between fiction and reality ("*de la communication olfactive,"* as the French would put it) is thin (Winkin, 2003). Wary of the fact that certain threats are less obvious than others, the researcher introduced the cyber-WMD concept as a primer to study and learn about a darker side of digital information technologies.

Internet as Terrorist Transport Vehicle of WMD

Some of the early indicators of the quiet transformation of the Internet as a potential terrorist transport vehicle of WMD include:

- The introduction of aroma-embedded information systems in multimodal human-computer interactions
- Advances in telemedicine applications involving pervasive and sensorial biochemical activities
- Ease and speed of information diffusion (via the Internet) related to terrorist activities (such as learning about bomb-making materials, terror-conditioning, and identifying potential targets)
- Worldwide access to potential victims in nanoseconds with relatively minimal financial resources or formal training

- Careless adoption of emergent technologies likely to be morphed into WMD
- Acknowledgement by many terrorist groups and their sympathizers of the opportunities offered by emerging digital information technologies and their documented intent to use such knowledge (i.e., Internet propaganda/information warfare)
- Formation of virtual teams and utilization of advanced computer simulations and diagrams to transfer very sophisticated knowledge (e.g., chemical processes or simulation of very complex reactions)
- The lack of interest by unwary defense and security officials to develop proper counter-intelligence[13] against the potentially dreadful cyber-WMD threat

In short, the recent waves of terrorist attacks reiterated the importance of the researcher's prescient mutation paradigm (Hyacinthe, 2005a & 2006a), compelling him to engage in action research (Kock *et al.*, 1997; Lau 1997) in order to address some of the key issues discussed herein. As such, the comparative analysis mentioned above was consistent with the primary purpose of this dissertation to offer a safer environment for emergent cyber-assisted olfaction technologies.

[13] The enemy might not always know when he is being watched, but he appears to know when he is not watched.

Table 4: Seven findings from the comparative data analysis

Findings of the Comparative Content Analysis
1. Emerging digital information technologies have the potential to transform the Internet and other critical network settings into a terrorist transport vehicle of WMD: a threatening cyber-WMD nexus.
2. Scientists from Europe, Asia, and the United States have very recently filed a significant number of patents (US5949522; US6524537; US6004516; US2004024043) seeking to extend human-computer interactions with the introduction of aroma-embedded information systems (such as scented emails, fragrance-embedded browsers, and other innovative forms of digital aroma diffusers). No comprehensive cyber-assisted olfaction security protocols have been reported.
3. Adopters of emergent technologies are likely to engage in cyber-assisted olfactory information exchanges through an array of digital devices with the potential to be morphed into WMD (by terrorists or other enemies). And there is an urgent need for innovative research studies that seek countermeasures against this potentially dreadful threat.
4. U.S. military experts from the Army War College (ADA326609), the Naval War College (ADA236609), the Air University (ADA407098), the Naval Post Graduate School (ADA365438), and the U.S. Marine Corps (ADA407502) acknowledged the imminence of the WMD threat on the U.S. soil and abroad. A large number of the reports focused on terrorism as the primary source of the WMD threat.
5. As the Polonium 210 incident in London suggests (Preliminary British Intelligence Report, 2006), airborne biochemical threats (not limited to direct terrorist acts) are mutating and the number of potential targets is increasing (e.g., aircrafts, subway systems, cruise ships, arenas, and even cell phones).
6. The academic literature on aroma-embedded information systems (with the exception of the lawyerly drafted patent publications) is very limited. In addition, the academic literature on possible threats to cyber-assisted olfaction technologies is virtually nonexistent.
7. Neither the military reports nor the patent applications discussed the threats associated with cyber-assisted olfaction technologies. There is a need for such discussions. This researcher has been actively engaged over the last five years in the construction of a model for safer cyber-assisted olfaction technologies (based on very early warnings).

DISCUSSION OF SURVEY RESULTS AND VALIDATION OF HYPOTHESES

This section describes the process and analysis related to the data collected with the goal of testing the hypotheses previously introduced in Chapter 1 and discussed in Chapter 4. The survey instrument comprised two major sections: The first section covered demographic information such as “major,” “academic level,” and

"gender." It was determined that age would not vary significantly enough to yield useful information in present situation. Consequently, age was not a factor in the analyses performed. To avoid superfluous data, the researcher did not collect any information related to the ethnic background of the respondents. The second section of the survey contained twenty one questions. Eighteen out of the twenty one (18/21) questions were used in the final analysis. Six questions were assigned to each factor (credibility, usefulness, and ease-of-use) according to categories established in Davis (1989) or Fogg (2003). The remaining three questions only played a supportive/reinforcement role to other questions.

Ten submissions contained mainly empty spaces and were therefore unusable. The demographic profiles of the usable responses are listed on Table 5. Descriptive statistics were computed for each of the eighteen questions and the results are summarized on Table 6. The researcher loaded the data collected into SPSS 15.0. The eighteen questions were all coded with numbers ranging from 1 (for "strongly disagree") to 5 ("strongly agree"). According to the SPSS-based data analysis (see Table 6), most of the respondents were males majoring in electronics (21/56=38%) and electrical engineering (30/56=55%). Based on the fact that the researcher sought for respondents (regardless of age or race) with the intellectual ability to interpret block-diagrams and understand basic design of digital information systems, the results of the demographic information confirmed the fact that a group representative of the targeted population (engineering students) was reached.

Table 5: Demographic information

Male	44	*Age*	Not Colleted
Female	12	*Race*	Not Collected
Graduate	9	*Geographic Location*	Southern USA
Undergraduate	40	*Major*	Engineering

The researcher launched a query for a maximum range of 100 cases (SPSS default). The range was appropriate since the final sample size (N=56) was inferior to 100. The preliminary observation of the dataset revealed a higher ratio (44/56=79%) of male than female (12/56= 21%) respondents (Table 5). As such, the findings were consistent with the conventional wisdom classifying engineering as a (historically) male- dominant discipline. Further analysis also revealed that 40/49=82% were undergraduate students and 9/49=18% were graduate students (see Figure 5 & APPENDIX H). One possible explanation for such "academic rank" disparity may be

the fact that the FAMU-FSU college of engineering program retains a lower number graduate students –suggesting that most of its alumni might have chosen lucrative positions over graduate degrees. Another possibility may be the fact that the researcher targeted densely populated classrooms – an atypical setting for graduate students. And lastly, seniors and graduate students might be unavailable because they are too busy preparing for graduation or senior projects. Why not? They might simply be tired of responding to surveys after so many of them. And perhaps they might have been discouraged by the lack of financial rewards for completing the survey.

HYPOTHESES AND TEST RESULTS

In essence, the researcher sought for empirical evidence to support the credibility of the proposed *MSCAO* and the overall argument that it would improve security and mitigate the harmful effects of potentially lethal bioactive substances. Accordingly, for each hypothesis, the researcher examined and discussed the differences between the variables (usefulness, ease-of-use, and credibility) in terms of their influence on the respondents' perceptions regarding the adoption of the proposed *MSCAO*. Thus, to avoid an overly exhaustive discussion of the findings, the researcher carefully used illustrative block-diagrams and tables to compress information that would otherwise require a tremendous amount of writing space and reading time. Further, in order to test the hypotheses, a series of t-tests, F-tests, and ANOVA analyses were performed under the following conditions:

H_1: *"Perceived Usefulness" and "Perceived Ease-of-use" are positively correlated to likely adoption of the MSCAO.*

As established in this dissertation, a level is considered to be significant if the associated mean score is superior to the midpoint value of 3.0 of the Likert scale (a score representative of a scenario where most of the respondents choose to agree or strongly agree). In relation to this hypothesis, the researcher provides a snapshot of the survey items (SI) involved below (see APPENDIX C):

SI#5: *I believe that this technology would be capable of reducing potential harms of biochemical threats*.

SI#11: *Overall, I believe that this technology would be useful for security and safety of cyber-olfaction technologies*.

SI#14: *I believe that it would be prudent for a user to adopt this technology for protection against a potential biochemical threat*.

SI#16: *I would trust these harm-reduction measures to make cyber-olfaction technologies (such as aromatic emails, automatic air fresheners, aroma-embedded printers) more acceptable to intended users*.

SI#21: *Overall, this technology would be easy-to-use as a harm-reduction solution against potential threats associated with cyber-olfaction technologies*.

Table 6: Classification by engineering majors

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Unidentified	1	1.4	1.8	1.8
	Electronics	**21**	**30.4**	**37.5**	**39.3**
	Electrical & Computer	**30**	**43.5**	**53.6**	**92.9**
	Mechanical	1	1.4	1.8	94.6
	Biomedical and Chemical	1	1.4	1.8	96.4
	Civil	2	2.9	3.6	100.0
	Total	56	81.2	100.0	
Missing	System	13	18.8		
Total		69	100.0		

According to the results obtained from SPSS (APPENDIX H), the mean score for usefulness was 3.6>3.0 compared to 3.5>3.0 for ease-of-use. As shown on Tables 10, &10b, both scores were greater than 3.0 [3.6> (usefulness) 3.5 (ease-of-use) >3.0].

Further analyses also showed a 67.2 % respondents' agreement (58% "agree" plus 9.2% "strongly agree") for usefulness suggesting thereby a positive influence of *perceived usefulness* on the users' intention to adopt the proposed model. Similarly, data related to *perceived ease-of-use* showed that 56.4 % (50.8% "agree" plus 5.6% "strongly agree") of the respondents supported the overall proposition that cyber-assisted olfaction technologies would be easy to use (Figure 12). The latter finding rather surprised the researcher who hypothesized that security and safety (i.e., perceived credibility) would have scored higher. This is a good example where the results of the survey instrument served as a correction tool against erroneous

assumptions. In synthesis, according to the information gathered and analyses performed, perceived usefulness and perceived ease-of-use were statically correlated (Table 8).

Table 7: Descriptive statistics for Hypothesis #1 (SPSS)

Ease-of-Use

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	7	1.9	**1.9**	1.9
	disagree	44	12.2	**12.2**	14.2
	neither	106	29.4	29.4	43.6
	agree	183	50.8	**50.8**	94.4
	strongly agree	20	5.6	**5.6**	100.0
	Total	360	100.0	100.0	

Usefulness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	9	2.5	**2.5**	3.1
	disagree	27	7.5	**7.5**	10.6
	neither	76	21.1	21.2	31.8
	agree	212	58.9	**59.1**	90.8
	strongly agree	33	9.2	**9.2**	100.0
	Total	359	99.7	100.0	
Missing	System	1	.3		
Total		360	100.0		

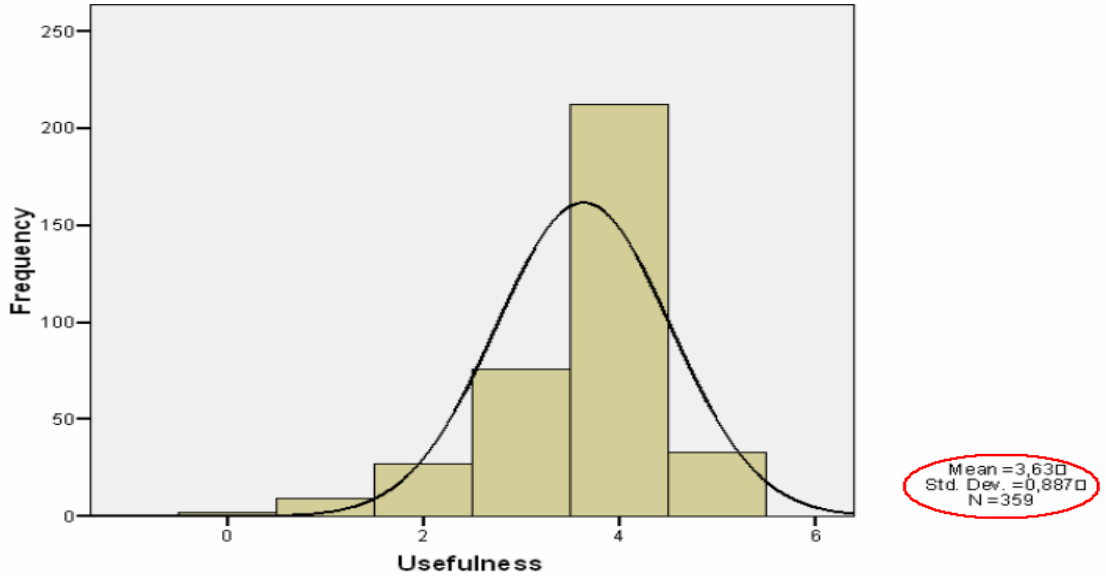


Figure 12: Histograms and sample mean scores

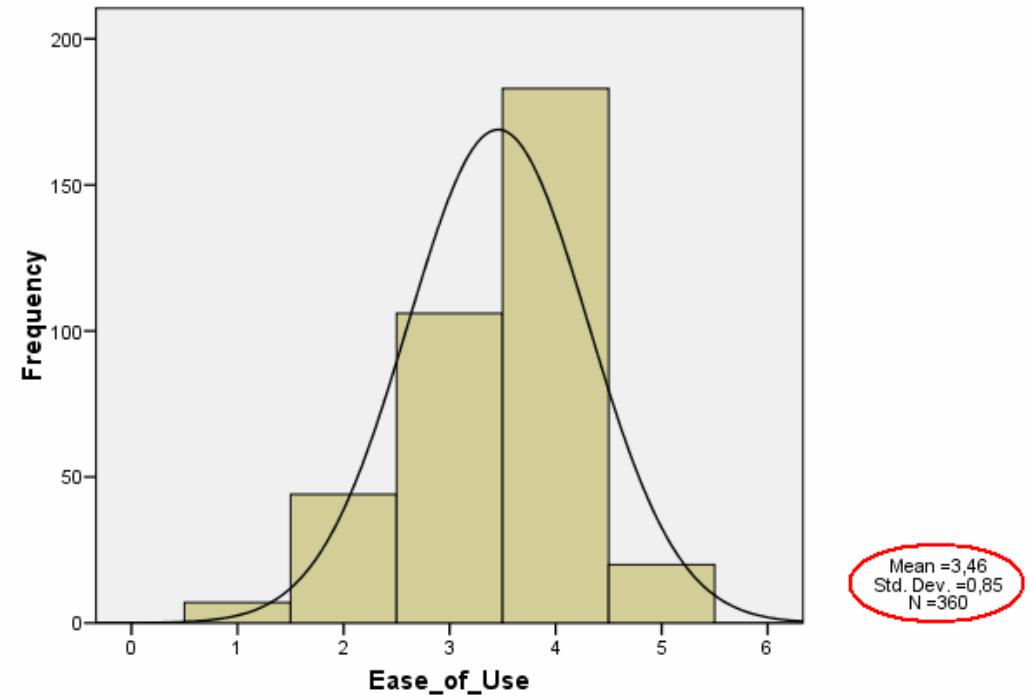


Figure 12: Histograms and sample mean scores (continued)

As the histograms of Figure 12 also suggest, the similarities persist in the behavior of the two curves. It is therefore reasonable to conclude that perceived usefulness and ease-of-use (both) have obtained scores significantly high to positively influence the adoption of the *MSCAO*. In other words, the level of disagreement (12%) is statistically insignificant compared to the level of agreement (50.8%). As the results of the t-test confirmed, H_1 has been proven and accepted (see Table 7 and Table 9).

Table 8: Correlations between constructs (SPSS)

		N	Correlation	Sig.
Pair 1	Credibility & Ease_of_Use	357	.318	.000
Pair 2	Credibility & Usefulness	356	.406	.000

Table 9: T-Test Results (H_1)

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Credibility	3.44	357	.942	.050
	Ease_of_Use	3.45	357	.852	.045
Pair 2	Credibility	3.44	356	.940	.050
	Usefulness	3.63	356	.890	.047

Paired Samples T-Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		Mean	Std. Deviation	Std. Error Mean
		Lower	Upper	Lower	Upper	Lower	Upper	Lower	Upper
Pair 1	Credibility - Ease_of_Use	-.014	1.051	.056	-.123	.095	-.252	356	.801
Pair 2	Credibility - Usefulness	-.185	.998	.053	-.289	-.081	-3.504	355	.001

H_2**:** *"Perceived Usefulness" is positively correlated to "Perceived Credibility" with regards to the likely adoption of the MSCAO.*

At the base of this hypothesis, the researcher used the equation below to determine the coefficient of the relation (Figure 13). In principle, two variables are said to be positively associated if, as X increases, the values of Y tend to increase. Two variables are said to be negatively associated if, as X increases, the values of Y tends to decrease. When no particular direction (neither positive nor negative) is shown, there is no linear association.

- The equation for the correlation coefficient is:

$$\rho_{X,Y} = \frac{Cov(X,Y)}{\sigma_X \cdot \sigma_Y}$$

where:

$$-1 \leq \rho_{xy} \leq 1$$

and:

$$Cov(X,Y) = \frac{1}{n}\sum_{j=1}^{n}(x_j - \mu_X)(y_j - \mu_Y)$$

Figure 13: General equation for correlation coefficient

Two separate methods and two different computer programs were utilized in this section. The researcher used the function "CORELL" (short of correlation) of Microsoft

Excel and processed the same dataset through SPSS 15.0 to obtain the same results displayed in Table 10.

Table 10: Correlation computed using SPSS (H_2)

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	Credibility & Ease_of_Use	357	.318	.000
Pair 2	Credibility & Usefulness	356	.406	.000

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Credibility	3.44	357	.942	.050
	Ease_of_Use	3.45	357	.852	.045
Pair 2	Credibility	3.44	356	.940	.050
	Usefulness	3.63	356	.890	.047

Paired Samples T-Test

		Paired Differences					t	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference		Mean	Std. Deviation	Std. Error Mean
		Lower	Upper	Lower	Upper	Lower	Upper	Lower	Upper
Pair 1	Credibility - Ease_of_Use	-.014	1.051	.056	-.123	.095	-.252	356	.801
Pair 2	Credibility - Usefulness	-.185	.998	.053	-.289	-.081	-3.504	355	.001

As shown on Table 10, for credibility and ease-of-use, t=-2.52 and p= .801/2=.400. Although both constructs positively influence the intention to adopt, the relation p> .05 indicates that the variables are not equally influencing the adoption the *MSCAO*. Simply stated, they are not affecting the "intent-to-adopt" with equal intensity.

For credibility and usefulness the relation p= (.001)/2 = .000<.05) suggests that the two constructs would influence the *MSCAO* at a closer rate than the other pair (i.e., credibility and ease-of-use).

To obtain more support and validate the results of the operations performed above, an F-test was also performed (using SPSS). A larger F-ratio (69.9) and smaller p-value (.ooo) are indicative of a smaller population standard deviation. In conclusion, the means of the constructs might be different but there is not enough evidence to deny their influence on the intention to adopt the proposed *MSCAO* (see Table 11).

Table 11: ANOVA between Credibility and Usefulness (SPSS)

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	46.326	1	46.326	69.864	.000(a)
	Residual	234.730	354	.663		
	Total	281.056	355			

a Predictors: (Constant), Credibility
b Dependent Variable: Usefulness

Table 12: Agreement Ratios for Hypothesis #2 (SPSS)

Credibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	14	3.9	**3.9**	3.9
	disagree	40	11.1	**11.2**	15.1
	neither	110	30.6	30.8	45.9
	agree	161	44.7	**45.1**	91.0
	strongly agree	32	8.9	**9.0**	100.0
	Total	357	99.2	100.0	
Missing	System	3	.8		
Total		360	100.0		

Usefulness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	9	2.5	**2.5**	3.1
	disagree	27	7.5	**7.5**	10.6
	neither	76	21.1	21.2	31.8
	agree	212	58.9	**59.1**	90.8
	strongly agree	33	9.2	**9.2**	100.0
	Total	359	99.7	100.0	
Missing	System	1	.3		
Total		360	100.0		

The need for further analysis and to foster understanding compelled the researcher to sort the data and regroup the information collected under two main categories “agree” in blue and “disagree” in red (Table 12). According to the latter classification scheme, the scores obtained for “strongly agree” & “agree” were computed together and the same was done for “disagree” & “strongly disagree.” After exporting the data from SPSS to Excel in order to produce a friendlier graphical user interface (Table 12), the results showed that the ratio (agree/disagree) was positive for both categories.

On the one side, the ratios were 4.16 (ease-of-use), 7.85 (usefulness), and 4.03 (credibility), clearly showing that the ratio (agree/disagree) was statistically greater than 1 for all three factors (Table 12)

On the other side, the ratios were 2.86 (ease-of-use), 4.33 (usefulness), and 2.29 (credibility), clearly showing that the ration agree/disagree was also statistically greater than 1 for all three factors.

In synthesis, based on the information presented above, a positive relationship appears to exist between perceived usefulness and perceived credibility. As such, in spite of a difference in magnitude, perceived usefulness and perceived credibility appear to have a positive influence on the adoption of the proposed *MSCAO*. H_2 has been tested, proven, and accepted (see Table 14).

H_3: *"Perceived Usefulness" is more important than "Perceived Ease-of-Use" when considering the likely adoption of the MSCAO*.

Through this hypothesis, it is predicted that the mean score of perceived usefulness would be greater than the mean score of perceived ease-of-use. Table 13 displays the results of the SPSS tests. Accordingly, the mean score of perceived usefulness (**3.63**) was higher than the mean score of ease-of-use (**3.46**). The probability of the sample data under the assumption that the null hypothesis is true (p value = .006) was lower than the alpha level **(.05)** set prior to data collection. Consequently, the null hypothesis was rejected and H_3 (supported by the data) was accepted.

In summary, this hypothesis was aligned with Davis' (1989) prediction that usefulness tends to score higher than ease-of-use. Davis' observation was proven to be true (once more) in this study. According to computations handled by SPSS, the mean score for perceived ease-of-use was **3.46**, a value statistically lower than **3.63** recorded for perceived usefulness (*usefulness > ease-of-use*). One logical interpretation of the latter results is that *usefulness* exerts a more positive influence (than *ease-of-use*) on the respondents' intent to adopt the *MSCAO*. Consequently, H_3 was accepted.

Table 13: Mean scores for usefulness, ease-of-use, and credibility

		Credibility	Ease_of_Use	Usefulness
N	Valid	357	360	359
	Missing	3	0	1
Mean		**3.44**	**3.46**	**3.63**
Std. Error of Mean		.050	.045	.047
Median		4.00	4.00	4.00
Std. Deviation		.942	.850	.887
Variance		.888	.722	.786

H_4: *"Perceived Credibility" is more important than "Perceive Ease-of-Use" when considering the likely adoption of the MSCAO.*

Wary of the magnitude of the anticipated threat, the researcher hypothesized that respondents would display a more positive attitude toward credibility (which accounts for trust and security) than ease-of-use. However, after testing and analyzing the results, there was no evidence to support the researcher's hypothesis (Table 13). In fact, *credibility* received a lower score with a mean of **3.44** (compared to **3.46** for ease-of-use). The probability of the sample data under the assumption that the null hypothesis is true (**p value = .006**) was lower than the alpha level **(.05)** set prior to data collection. Therefore, the null hypothesis was accepted and H_4 was rejected.

H_5**:** *Electrical engineering students display a more positive attitude toward the credibility of the MSCAO than electronic engineering students.*

To test this hypothesis, the researcher built a new dataset, which consisted of the two major groups of interest (Table 6): Electronic Engineering students (38% of the sample) and Electrical Engineering students (57% of the sample) were analyzed. The electronic engineering students account for most of the students enrolled in the technical program at FAMU, which focuses primarily on the formation of *technicians* as opposed to research engineers. The electrical engineering students are enrolled in the joint FSU-FAMU engineering school (e.g., traditional electrical engineering program), which focuses primarily on teaching and research and development. The new dataset was established according to the requirements of the t-test. Subsequent to the data manipulation using SPSS, the researcher concluded that there was no significant difference in the attitudes of the two groups to support the hypothesis. Therefore, H_5 was rejected.

Table 14: Summary of test results for the five hypotheses

Hypotheses	H_1	H_2	H_3	H_4	H_5
Validation	Accepted	Accepted	Accepted	Rejected	Rejected

Limitations

The researcher utilized expert opinions both for pilot testing and post-survey analysis and decided not to conduct follow-up interviews for reasons including (a) the theoretical aspect of the proposed model did not impose a strict feedback format, (b) most of the respondents would not be available during the summer semester that followed data collection, (c) too much time would have elapsed between data collection and follow-up interview (if the researcher were to wait until the following fall semester), (d) tacit knowledge was strategically infused into the analysis through the researcher's direct interactions (via open feedback) with experts in the areas of biochemical defense, terrorism, information warfare, information policy, hedonics, health informatics, and computer science & engineering, and (e) the comparative analysis between the patent search and the declassified reports yielded a substantial amount of qualitative data to complement the quantitative survey data. The declassified military reports were restricted to the United States. Although the threats appear to be worldwide, the views and counterstrategies might be different from Asian or European perspectives. As the researcher anticipated, the absence of a hands-on trial of the system accounted for another limitation (inherent to most theoretical or conceptual models).

CHAPTER SUMMARY

The processes adopted and the analyses performed above have been supported by proven theories and reliable instruments. As it is the case for any ambitious endeavor of this caliber, the analysis performed above was not immune to imperfections and surprises. For instance, more sophisticated statistical analysis could be employed to provide a deeper understanding of attitudes towards the proposed MSCAO.

In spite of the limitations discussed, the data collected from the different methods were compiled and synchronized to display a holistic picture of the findings. As demonstrated above, the researcher monitored the results from each query technique and each test in terms of their relationship to the proposed *MSCAO*. For instance, t-tests were performed through SPSS while correlations were examined using Microsoft

Excel. The analyses were based on users' perceptions, which are naturally difficult to measure.

Even under these very challenging conditions (researcher's imperfections, procedural restrictions, and other inherent limitations to this type of research), the *MSCAO* emerged as an invaluable framework, which has been supported by established research protocols and theoretical concepts applied to technology adoption studies. A comprehensive framework to understand various aspects of cyber-assisted olfaction technologies should also account for related threats and dangerous applications. Thus, the researcher listed seven findings of the comparative content analysis (Table 4) and outlined what he considered to be the early warnings of the quiet transformation of the Internet as a terrorist transport vehicle of WMD. Further, he recapitulated the test results of the five hypotheses on Table 14.

As a potential support to the prototype phase of the system, the post-analysis snapshot below captured the variables and the magnitude of their influence on the respondents' perceptions related to the *MSCAO* (Figure 14).

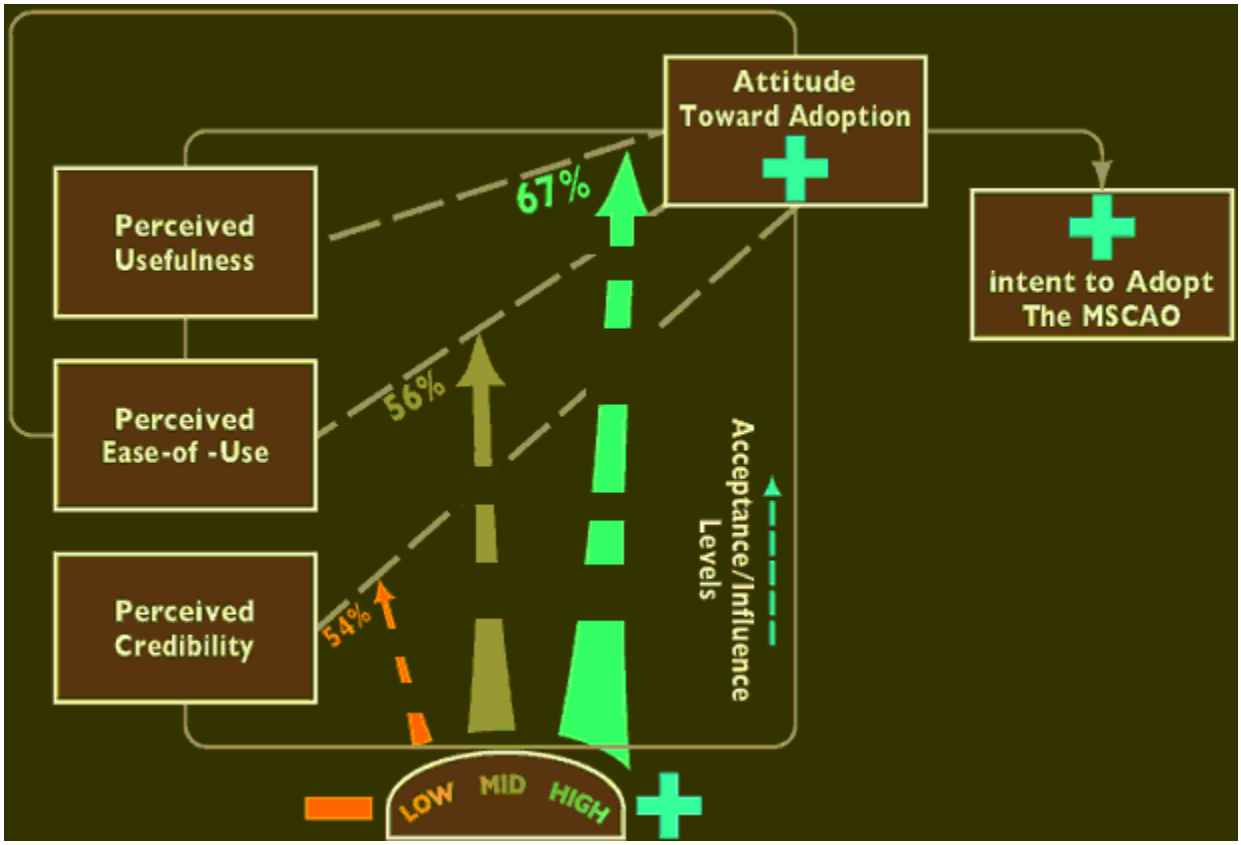


Figure 14: Observed acceptability of the MSCAO

CHAPTER V: PRESCRIPTIONS AND CONCLUSIONS

WARNINGS, LIMITATIONS, AND FURTHER RESEARCH

Cyber-assisted olfactory communications fall within the realm of multimodal human-computer interactions. And the discussions held throughout this dissertation support the researcher's claim that cyber-assisted olfaction is likely to be accepted as a common “type” of human-computer interaction in the future. The primary purpose of this dissertation was to examine users’ adoption of emergent technologies and to use the results to present a model for safer cyber-assisted olfactory information exchanges in various settings. On the one side of the spectrum, the research analysis entailed users’ attitudes regarding the adoption of emergent cyber-assisted olfaction technologies. On the other side, the researcher focused particularly on the level of acceptability of the proposed security and safety protocols related to cyber-assisted olfactory information exchanges.

Although the survey focused on a group of engineering students, the researcher acknowledged the potential threats associated with careless adoption of emergent technologies as well as the adoption of such technologies to spread terror. Based on the prescriptive nature of this dissertation (e.g., a MSCAO), the researcher issued warnings and made several recommendations related to these threats.

Though it supported the research problem stated in Chapter 1, the literature did not reveal any previous attempts to offer the type/level of information security proposed in here. Through the proposed MSCAO, the researcher sought to contribute to the existing body of knowledge associated with the adoption of emergent technologies and particularly to aroma-embedded information systems (as they relate to olfactory information warfare and national defense and security).

The researcher’s interactions (Hyacinthe, 2006a & 2006b; Hyacinthe and Anglade, 2007, Hyacinthe *et al.*, 2007) with experts in the areas of information policy, national defense, information warfare, terrorism, and biochemical warfare offered new opportunities to examine the students’ perceptions regarding the proposed model and to opine on their intent to adopt emergent digital information technologies.

In Chapter 2, the researcher built on prior discussions addressing olfactory displays in virtual reality environments and entertainment, multimodal interfaces related to affective technologies, and aroma therapy to substantiate, through the literature reviewed, his proposed model. In summary, the *MSCAO* amounts to a new,

comprehensive, flexible framework to understand various aspects of aroma-embedded information systems, and that may be usefully applied to a wide range of systems (from standard to micro- and nano- apparatuses).

The analytical findings were based on previous instruments of reliable technology adoption studies and procedures developed specifically for the current research. The theoretical concepts and methodology adopted have been discussed in Chapter 1 and Chapter 3. The researcher both described and defended the methodology chosen for this research in Chapter 3. He also investigated the possible ways of approaching the various research questions with the support of prior research methods and techniques. Chapter 3 concluded with an exposé of the major tasks and important missions accomplished towards the realization of the overall theoretical framework upon which the research was built. Accordingly, the survey instrument was discussed. And following rigorous testing using SPSS, the validity of the constructs was deemed acceptable.

In effect, a thorough analysis of the measurement items (scales) showed that measures were reliable and that constructs had acceptable convergence and discriminant validity. Nonetheless, there are still issues of relevance to the internal and external validity of the present study that may be resolved through further investigation.

WARNINGS AND PRESCRIPTIONS

Historically, exploratory reports are meticulously deciphered and widely publicized only after the threats they warn about have been manifested. For example, in the United States, government officials have been fortunate enough to receive warnings regarding the most dreadful catastrophes but often failed to act in a timely manner (APPENDIX K).

The international intelligence community needs to address issues of security and information policies related to the design and implementation of aroma-embedded information systems. The world can not afford another scenario of "*known worms go free*" or "*lack of actionable intelligence.*" The stakes are too high this time around. This cyber-WMD threat goes beyond the reversible matters of corrupted files and network intrusions.

The issues covered in this dissertation are not limited (solely) to the national security of the United States. It is likely that one of its allies will take notice and act against these threats before they translate into attacks. In the end, the United States

may still benefit from such preventive actions (i.e., the protection of aircrafts against bioactive substances discussed two years prior to the "*Polonium 210*" and the "*liquid explosive*" incidents in London). In hindsight, if earlier warnings (Hyacinthe, 2005 & 2006) were taken seriously, measures currently taken against liquid explosives and other threats inside aircrafts would have preceded the latter London incidents.

The potential of terrorists and other enemies to use the Internet and/or other digital information technologies as transport vehicles of weapons of mass destruction (WMD) was exposed. The researcher established and substantiated the fact that such a threat may involve cyber-assisted biochemical transactions, which can be performed through olfactory information exchanges, to attack civilian and military targets anytime.

As a product of a four-year investigation wherein the researcher went through a rich archive of declassified U.S. military reports and a selective list of patent applications, the dissertation tackled the problem of careless adoption of unsafe technologies –susceptible to be morphed into a dreadful cyber-WMD nexus.

Accordingly, the researcher examined and explained several aspects of cyber-assisted olfaction technologies as they relate to the replication of the human sense of smell by computer systems. Through several interesting examples, the researcher explained the process of stimulation of human olfactory receptors by computer-emitted biochemical or aromatic particles. Further discussions also covered the use of olfaction-based biosensors, known as electronic noses, to detect chemical plumes (aroma or warfare agents) for a wide range of applications. Among other applications, multimodal, affective human-computer interactions involving scented emails, aroma therapy, and olfaction-based marketing were considered.

Based on the analysis performed, credibility, ease-of-use, and usefulness received scores significant enough to be considered as positively influencing the adoption of the proposed *MSCAO*. The results of this study were similar to other studies involving a different set of demographic groups. For instance, several studies (Davis *et al.*, 1989; Keil *et al.*, 1995; Satzinger and Olfman, 1995; Taylor and Todd, 1995; Igbaria *et al.*, 1996) found perceived usefulness to have the strongest influence. In essence, the respondents found the *MSCAO* to be a very useful proposition and expressed a significantly high level of need for harm-reduction and cyber security measures against potential threats. Extrapolating from the findings reported herein, the researcher concluded that users are likely to adopt an

emergent technology that is useful, easy-to-use, and that offers credible harm-reduction measures.

FURTHER RESEARCH AND PRESCRIPTIONS

Recommendations for further research also include (1) the exploration of cyber-assisted degustation, (2) a comparative data analysis between *military experts* and *engineering students* using a similar survey instrument, (3) an experimental research with the primary objective to build a working prototype, (4) follow-up studies that look at students' friction[14] about the use of aroma-embedded information systems, and (5) an investigation of the potential side effects of a selective list of neutralizing substances. As Dr. Burke suggested, the substitution of credibility by anxiety could be an interesting setup to explore users' fear of the threats associated with aroma-embedded information systems. In future research, institutions of different missions and sizes may be compared. For example, the data already collected by the researcher may be compared with data collected from a military institution or an industrial setting for further analysis.

CONCLUSION

Early adopters are embracing emergent technologies faster than ever (Waters, 2007). Unfortunately, with the widespread diffusion of digital information technologies, the adoption of emergent technologies to spread terror is likely to grow with dreadful consequences. As Littleton (2005) noted in the abstract of his military thesis (from the Naval Postgraduate School, Monterey, California):

> Terrorism in the information age will consist of conventional terrorism, in which classic weapons (explosives, guns, etc.) will be used to destroy property and kill victims in the physical world; technoterrorism, in which classic weapons will be used to destroy infrastructure targets and cause a disruption in cyberspace; and cyberterrorism, where new weapons (malicious software, electromagnetic and microwave weapons) will operate to destroy data in cyberspace to cause a disruption in the physical world.

As described in Chapter 3, survey questionnaires were gathered from 70 participants located at the FSU/FAMU College of Engineering, Tallahassee, Florida. The study findings (Chapter 4) provided substantial support to the proposed security and safety model. Perceived usefulness (67%) was identified as the principal

[14] For example, *anxiety* is a very popular construct used in technology adoption research to determine friction of technology adopters.

determinant of the respondents' intention to adopt the proposed model. Although it was less substantial than perceived usefulness, perceived ease-of-use (56%) appeared to have a greater influence on the *MSCAO* than perceived credibility (54%). More importantly, the respondents' positive attitude regarding the extended construct (perceived credibility) and the accentuated importance of perceived usefulness corresponded to the dissertation's aim to examine users' adoption of emergent technologies and to present a model for safer cyber-assisted olfactory information exchanges in various settings. The *MSCAO* is offered as a harm-reduction measure against a potentially dreadful threat to a wide range of targets often designated as *terrorist targets*.

Chapter 4 also covered the interpretation of the results during which the hypotheses were validated (accepted or rejected). Overall, the results displayed a positive influence of all three factors (perceived usefulness, perceived ease-of-use, and perceived credibility) on the respondents' intent to adopt the *MSCAO*. Based on the established five-grade Likert scale, the respondents appeared to agree (more than they disagree) to the proposed model (Figure 15).

According to Figure 12 and Figure 15, the agree/disagree ratios were 4.16 (for ease-of-use), 7.85 (for usefulness), and 4.03 (for credibility). And strongly agree/strongly disagree ratios were 2.86 (for ease-of-use), 4.33 (for usefulness), and 2.29 (for credibility). As clearly shown on Table 11 and Figure 15, the overall agree/disagree ratio was statistically greater than 1 for all three factors. In fact, within the parameters set by the researcher, it was possible to obtain a quotient (agree/disagree) greater than one (1) for each variable examined (signaling thereby an early confirmation of positive influence of the variables on respondents' intent to adopt the proposed *MSCAO*). Note that Figure 15 displays the constructs as "factors" under the following coding scheme: Perceived Credibility (PC), Perceived Usefulness (PU), and Perceived Ease-of-Use (PEOU).

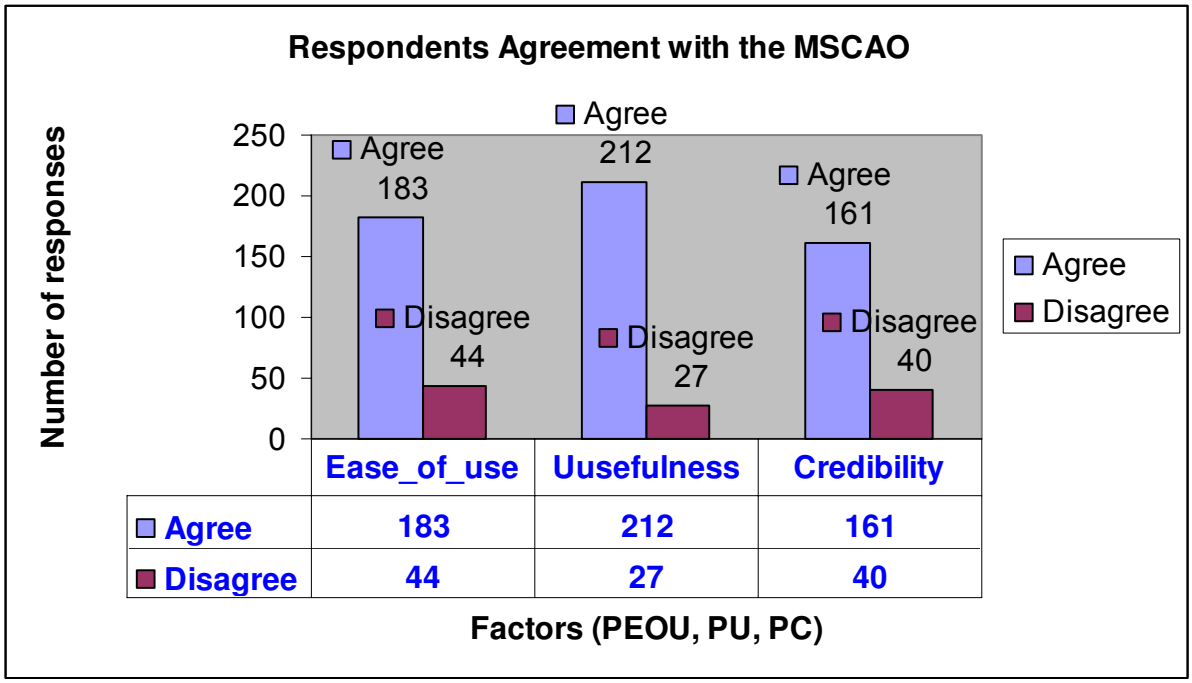


Figure 15: Agreement/Disagreement to the *MSCAO*

Though the researcher originally hypothesized that credibility would score higher than usefulness and higher than ease-of-use, a different picture emerged from the data analysis –compelling him to draw a post-analysis diagrammatic illustration that reflects the respondents' responses (Figure 14). The findings remain consistent with the researcher's general proposition that olfactory information exchanges (e.g., scented emails and olfaction-based marketing) will have a greater success, if a fail-safe system (such as autonomous neutralization of unwanted biochemical substances) is installed between the user and the system.

As a result, preventive physical cyber protocols have been introduced as an important factor of 21st century information security. Among other designs, the microfluidics suppressor (see APPENDICES D&E) exemplifies the breadth and depth of the *MSCAO*'s spectrum. The microfluidics suppressor was sought for the design of safer printers, fax machines, ink/toner cartridges, and other at-risk information technologies (i.e., aroma-embedded and chemically charged devices). The MSCAO may be adapted to intelligence foresight analysis, biochemical defense, and global security and defense of the most critical infrastructures.

Thus, largely supported by Everett Rogers' innovation diffusion theory and Fred Davis' technology acceptation model, the researcher went beyond the aphorism of "smell-o-vision" to offer a fertile ground for a new, comprehensive, and flexible framework to understand many aspects of emergent cyber-assisted olfactory

information systems that can be usefully applied to a wide range of auxiliary information systems (i.e., standard, micro, and nano devices). In relation to national security and defense, the MSCAO can be usefully applied in subway systems, aircrafts, cruise ships, and various mixing/distribution systems (i.e., water systems and chemical plants) to automatically detect and neutralize a bio or chemical threat. Many military applications are also anticipated for emerging urban warfare and emergency rescue operations using such devices as miniature robots and NAVs (APPENDIX G). The evolution of MEMS will continue to influence this widely adopted computers-as-weapons paradigm (as biologically-inspired systems are being developed and tele-guided miniature robots are being produced with capabilities to disperse lethal doses by crawling or flying).The danger has existed since the late 1930's. The scale might be all that has been modified from a 1944 design of a UAV, which was intended to disperse deadly airborne bioactive substances, according to U.S. intelligence accounts (APPENDIX F).

In sum, common wisdom would dictate that the design and development of UAVs and NAVs be done in parallel with very efficient autonomous biochemical decontamination systems, for the 'darker side' of the evolution of MEMS might soon produce Bio-NAVs too dangerous and too sophisticated to be countered by intelligent image recognition or signal 'jamming' techniques. The potential misuse of cybernetics as a biochemical warfare amplifier (in the near future) is real. The likely adoption by non-traditional and paramilitary groups of this reality and the resulting consequences should be further investigated. This obvious race towards computer-weapon singularity will intensify as the world flattens and new knowledge continues to spread in nanoseconds through creative media and innovative channels to a new class of enemies.

May the proposed MSCAO serve as a fertile ground for the acquisition of better understanding, creation of meta-knowledge, exploitation of new discoveries, and particularly the implementation of stealthier security protocols related to users' adoption of aroma-embedded information systems and devices!

APPENDIX A: FSU HUMAN SUBJECTS APPROVAL LETTER

Office of the Vice President For Research
Human Subjects Committee
Tallahassee, Florida 32306-2742
(850) 644-8673 · FAX (850) 644-4392

APPROVAL MEMORANDUM

Date: 11/30/2006

To:
Berg P. Hyacinthe
MC 2100

Dept.: **INFORMATION STUDIES**

From: **Thomas L. Jacobson, Chair**

Re: **Use of Human Subjects in Research**
User Adoption of Emergent Technologies: The Case of a Proposed Lab-on-Chip Model for Safer, Cyber-Assisted Olfactory Information Exchanges in Standard and Micro Systems

The forms that you submitted to this office in regard to the use of human subjects in the proposal referenced above have been reviewed by the Secretary, the Chair, and two members of the Human Subjects Committee. Your project is determined to be Exempt per 45 CFR § 46.101(b) 4 and has been approved by an accelerated review process.

The Human Subjects Committee has not evaluated your proposal for scientific merit, except to weigh the risk to the human participants and the aspects of the proposal related to potential risk and benefit. This approval does not replace any departmental or other approvals, which may be required.

If the project has not been completed by **11/28/2007** you must request renewed approval for continuation of the project.

You are advised that any change in protocol in this project must be approved by resubmission of the project to the Committee for approval. Also, the principal investigator must promptly report, in writing, any unexpected problems causing risks to research subjects or others.

By copy of this memorandum, the chairman of your department and/or your major professor is reminded that he/she is responsible for being informed concerning research projects involving human subjects in the department, and should review protocols of such investigations as often as needed to insure that the project is being conducted in compliance with our institution and with DHHS regulations.

This institution has an Assurance on file with the Office for Protection from Research Risks. The Assurance Number is IRB00000446.

Cc: Dr. John Gathegi
HSC# 2006.0993

APPENDIX B: FAMU HUMAN SUBJECTS APPROVAL LETTER

Florida Agricultural and Mechanical University
Tallahassee, Florida 32307-3100

Excellence with Caring

INSTITUTIONAL REVIEW BOARD

Telephone: (850) 412-5246
Fax: (850) 412-5012

APPROVAL MEMORANDUM

TO: Dr. Yves J. Anglade
Engineering Sciences and Technology

FROM: C. Perry Brown, DrPH
Chair, Institutional Review Board (IRB)

DATE: January 29, 2007

RE: "User Adoption of Emergent Technologies: The Case of a Proposed Lab-on-Chip Model for safer, Cyber-Assisted Olfactory Information Exchanges in Standard and Micro System" **(007-06)**

The Florida A&M University Institutional Review Board (IRB) has reviewed and approved the above name project and no other revisions are necessary.

The IRB has not evaluated your project for scientific merit, except to weigh the risk to the human participants and the aspects of the proposal related to potential risk and benefit. This approval does not replace any departmental or other approvals, which may be required.

If the project has not been completed by **January 29, 2008** you must request a renewed approval for continuation of this project.

You are advised that any changes in the protocol in this project must be resubmitted to the committee for approval. Also, the principal investigator must promptly report, in writing, any unexpected problems causing risks to research subjects or others.

The institution has an Assurance on file with the Office for Human Research Protection. The Assurance Number is **FWA00005391**.

APPENDIX C: INFORMED CONSENT FORMS AND SURVEY INSTRUMENT

CONSENT LETTER

July 28, 2006

Dear Dr. Anglade,

My name is Berg P. Hyacinthe. I am a PhD candidate from the College of Information at Florida State University. I am interested in exploring the information technology adoption phenomenon among Electronic Engineering students in your department. There is no published work that looks at how Electronic Engineering students perceive the design and implementation of aroma-embedded information systems. The future of such systems is highlighted in many patent applications (published and in press). More importantly, the potential danger associated with such systems makes it imperative that engineering students are exposed early to the evolution of this new type of information exchanges that will shape the way information systems are designed, secured, and implemented in the future.

Your participation in this new endeavor will create an opportunity for your students and your institution to explore the technology that promises to extend the definition of information systems and human computer interactions.

In particular, I am seeking for your approval to administer the attached survey to students enrolled in your Electronic Engineering program. The survey contains a demographic section and technology adoption section. A follow up interview shall be administered to a few selected participants.

Students can expect to spend no more than ten minutes completing the questionnaire. Completing the survey might be very easy to do because you simply place a tick in the relevant box. Once the survey is completed, it can be submitted automatically via the web space provided to the students. To maintain anonymity, students' name will not appear on the survey and their responses will not be shared with anyone else (but to a four-member doctoral dissertation committee). These procedures are meant to protect the confidentiality of responses. There are no known risks involved with participation. Moreover, during publication and oral reports, your institution will be referenced as a four-year state university in southern United States.

Students' participation in this study is voluntary. If a student chooses not to participate or to withdraw from the study at any time, there will be no penalty. The survey will not be used for academic grades. Although the results of the research study may be published, confidentiality will be retained.

If you have any questions concerning this research study, please call me at 954-652-9966 or e-mail me at bph02@fsu.edu. The results of this survey will form part of the discussions in a dissertation to be presented in partial fulfillment of the PhD. Program in the College of Information at Florida State University. Your return of completed surveys will be considered as your consent to participate.

Sincerely,

Berg P. Hyacinthe, Ph.D. Candidate

INFORMED CONSENT FORM

Please indicate your consent for the following:

□ I give my consent to participate in the above study. I understand that the information collected during the project will be kept by the researcher in a locked filing cabinet at Florida State University. The researcher will use the information of a doctoral dissertation and will destroy the recorded information by December 31, 2011.

□ I give my consent to be contacted for a voluntary follow-up interview of about 20 minutes.

Student Name _____ Date _____

Student Signature _____

This study has been approved by the Florida State University Institutional Review Board (**Protocol# IRB 446**). If you have any questions about your rights as a subject/participant in this research, or if you feel you have been placed at risk, you can contact the Chair of the Human Subject Committee, Institutional Review Board, through the Vice President for the Office of Research at (850) 644-8633. The results for each participant will be kept confidential to the extent permitted by law.

SURVEY INSTRUMENT

1. I would trust this technology to provide cyber-olfaction security for *entertainment and E-commerce purposes*.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

2. I believe that this technology would be easy to adopt for *entertainment and E-commerce* purposes.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

3. I believe that this technology would have a *positive impact on the popularity* of cyber-olfaction technologies.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

4. I believe that *integration of this technology with other compatible systems* (such as existing detection and warning systems) would not be difficult.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

5. I believe that this technology would be *capable* of reducing potential harms of biochemical threats.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

6. I would *accept* a free trial of "aroma-embedded messages" with my cell phone only if these security measures (proposed by this technology) are built-into the phone system.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

7. I believe that it would be easy to *learn the features and acquire new skills* associated with this technology.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

8. I would trust this technology to provide safety and security in *small and large scale cyber-olfaction systems.*

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

9. I believe that this technology would be *efficient* to counter potential bio-terrorism threats.

   Unlikely |----------| |----------| |----------| |----------| |----------| Likely
   strongly disagree disagree neither agree strongly agree

10. Overall, I believe that this technology would be *useful* for security and safety of cyber-olfaction technologies.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

11. I believe that this technology would be easy to *customize to various needs and personal preferences*.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

12. I believe that this technology would be useful to general users for *entertainment and E-commerce purposes***.**

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

13. I believe that it would be easy for potential users to *interact with this technology*.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

14. I believe that it would be *prudent* for a user to adopt this technology for protection against a potential biochemical threat.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

15. I believe that this technology would be useful for security in *small and large scale cyber-olfaction systems***.**

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

16. I would *trust these harm-reduction measures* to make cyber-olfaction technologies (such as aromatic emails, automatic air fresheners, aroma-embedded printers) more acceptable to intended users.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

17. I believe that it would be easy for this technology to provide safety and security in *small and large scale cyber-olfaction system*.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

18. I believe that this technology would be an *improvement* to existing cyber-olfaction technologies (such as automatic air fresheners and even ink-jet printing devices).

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

19. Overall, this technology would be an *easy-to-use harm-reduction solution* against potential threats associated with cyber-olfaction technologies.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

20. I believe that this technology would *increase user confidence* about using cyber-olfaction technologies.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

21. I believe that it would be easy to *learn about the operational and setup features* of this technology.

Unlikely |----------| |----------| |----------| |----------| |----------| Likely

strongly disagree disagree neither agree strongly agree

APPENDIX D: ABSTRACTS OF REVIEWED PATENTS

US 20040204043A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2004/0204043 A1**

Wang et al. (43) **Pub. Date: Oct. 14, 2004**

(54) **INFORMATION APPARATUS WITH INTERACTIVE SCENT INTERFACE**

(76) Inventors: **Hwai-Ming Wang**, Taipei City (TW); **Yao-Chon Tsai**, Taipei City (TW); **Feng-Zen Wu**, Taipei City (TW)

Correspondence Address:
NAIPO (NORTH AMERICA INTERNATIONAL PATENT OFFICE)
P.O. BOX 506
MERRIFIELD, VA 22116 (US)

(21) Appl. No.: **10/065,569**

(22) Filed: **Oct. 31, 2002**

(30) **Foreign Application Priority Data**

Aug. 29, 2002 (TW)..... 091119724

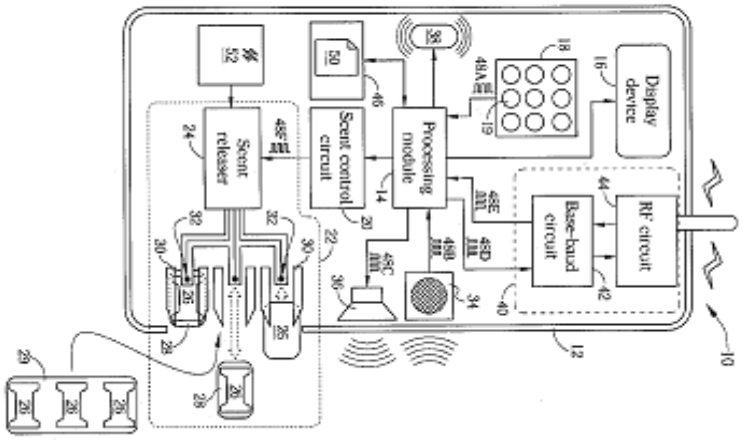
Publication Classification

(51) **Int. Cl.**[7] **H04B 1/38**; H04M 1/00

(52) **U.S. Cl.** **455/556.1**; 455/575.1; 455/90.1

(57) **ABSTRACT**

An information processing apparatus with an interactive scent interface comprises a housing, a processing module installed in the housing for controlling the information processing apparatus, an input module installed in the housing and electrically connected to the processing module for receiving input signals to generate corresponding control signals and for transmitting the corresponding control signals to the processing module. A display device is installed in the housing and electrically connected to the processing module for transforming information transmitted from the processing module into video data and for displaying the video data. A scent control circuit is also installed in the housing and electrically connected to the processing module for generating a scent control signal and a scent releasing module is installed in the housing and electrically connected to the scent control module for releasing scent particles according to the scent control signal.



US 20030158459A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0158459 A1**

Tucker (43) **Pub. Date: Aug. 21, 2003**

(54) **ENHANCED FORMULATIONS FOR NEUTRALIZTION OF CHEMICAL, BIOLOGICAL AND INDUSTRIAL TOXANTS**

(76) Inventor: **Mark D. Tucker**, Albuquerque, NM (US)

Correspondence Address:
PEACOCK MYERS AND ADAMS P C
P O BOX 26927
ALBUQUERQUE, NM 871256927

(21) Appl. No.: **10/251,569**

(22) Filed: **Sep. 20, 2002**

Related U.S. Application Data

(63) Continuation-in-part of application No. 09/607,586, filed on Jun. 29, 2000, which is a continuation-in-part of application No. 09/109,235, filed on Jun. 30, 1998, now abandoned.
Continuation-in-part of application No. 09/952,940, filed on Sep. 14, 2001, which is a continuation-in-part of application No. 09/607,586, filed on Jun. 29, 2000.

(60) Provisional application No. 60/326,508, filed on Oct. 1, 2001. Provisional application No. 60/334,271, filed on Nov. 30, 2001. Provisional application No. 60/387,104, filed on Jun. 7, 2002. Provisional application No. 60/146,432, filed on Jul. 29, 1999.

Publication Classification

(51) **Int. Cl.**[7] **A62D 3/00**

(52) **U.S. Cl.** **588/200**

(57) **ABSTRACT**

An enhanced formulation and method of making that neutralizes the adverse health effects of both chemical and biological compounds, especially chemical warfare (CW) and biological warfare (BW) agents, and toxic industrial chemicals. The enhanced formulation according to the present invention is non-toxic and non-corrosive and can be delivered by a variety of means and in different phases. The formulation provides solubilizing compounds that serve to effectively render the chemical and biological compounds, particularly CW and BW compounds, susceptible to attack, and at least one reactive compound that serves to attack (and detoxify or kill) the compound. The formulation includes at least one solubilizing agent, a reactive compound, a bleaching activator and water.

US006820012B2

(12) **United States Patent**
Sunshine

(10) **Patent No.: US 6,820,012 B2**
(45) **Date of Patent: Nov. 16, 2004**

(54) **COMPUTER CODE FOR PORTABLE SENSING**

(75) Inventor: **Steven A. Sunshine**, Pasadena, CA (US)

(73) Assignee: **Smiths Detection-Pasadena, Inc.**, Pasadena, CA (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **10/464,690**

(22) Filed: **Jun. 17, 2003**

(65) **Prior Publication Data**

US 2003/0216869 A1 Nov. 20, 2003

Related U.S. Application Data

(63) Continuation of application No. 09/703,467, filed on Oct. 31, 2000, now Pat. No. 6,606,566.
(60) Provisional application No. 60/164,022, filed on Nov. 4, 1999, provisional application No. 60/162,683, filed on Nov. 1, 1999, and provisional application No. 60/188,307, filed on Mar. 10, 2000.

(51) **Int. Cl.**[7] **G06F 13/14**
(52) **U.S. Cl.** **702/22**; 702/30; 702/31; 702/120; 702/122
(58) **Field of Search** 702/22, 30, 31, 702/120, 122, 183, 188, 109, 177; 435/6; 600/300, 345; 606/181

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,528,363	A		6/1996	Fachinger et al. 356/326
5,554,539	A	*	9/1996	Chadney et al. 436/8
5,571,401	A		11/1996	Lewis et al. 205/787
5,675,070	A		10/1997	Gelperin 73/23.34
5,697,326	A		12/1997	Moitram et al. 119/174
5,788,833	A		8/1998	Lewis et al. 205/787
5,790,977	A		8/1998	Ezekiel 702/122
5,807,701	A		9/1998	Payne et al. 435/34
5,891,398	A		4/1999	Lewis et al. 422/82.02
6,085,576	A		7/2000	Sunshine et al. 73/29.01
6,134,504	A	*	10/2000	Douglas et al. 702/31
6,175,752	B1	*	1/2001	Say et al. 600/345
6,234,006	B1		5/2001	Sunshine et al. 73/29.01
6,263,458	B1		7/2001	Miller et al. 714/47
6,329,139	B1	*	12/2001	Nova et al. 435/6
6,418,783	B2		7/2002	Sunshine et al. 73/29.01
6,422,061	B1		7/2002	Sunshine et al. 73/29.01
6,450,008	B1		9/2002	Sunshine et al. 73/23.34
6,592,822	B1	*	7/2003	Chandler 422/82.05
2002/0149466	A1		10/2002	Sunshine et al. 338/34
2002/0152037	A1		10/2002	Sunshine et al. 702/23

FOREIGN PATENT DOCUMENTS

EP	0 789 239	A1	8/1997
EP	0 943 992	A2	9/1999
GB	2342171	A	4/2000
WO	WO 99/14882		3/1999
WO	WO 99/47905		9/1999
WO	WO 01/69186	A1	9/2001

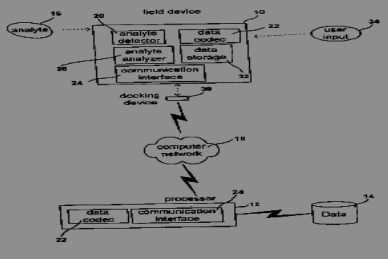
* cited by examiner

Primary Examiner—Marc S. Hoff
Assistant Examiner—Felix Suarez
(74) *Attorney, Agent, or Firm*—Foley & Lardner LLP

(57) **ABSTRACT**

The present invention relates to a computer program product or code in memory for detecting and transmitting sensory data from a portable field device **10** to a processor **12** via a computer network **10** for analytic purposes. The product includes a code directed to capturing analyte data pertaining to an unknown analyte using a field device **10**. The product further includes a code directed to encoding the captured analyte data and transmitting the encoded analyte data via a computer network **18** to a processor **12** for analysis. The product also includes a code directed to performing an analysis of the captured analyte data at a remote location by the processor **12** using data of known analytes retrieved from an electronic library **14**. This code and others can be used with the present invention to perform the functionality described herein as well as others.

9 Claims, 8 Drawing Sheets



US006004516A

United States Patent [19]

Rasouli et al.

[11] **Patent Number: 6,004,516**

[45] **Date of Patent: Dec. 21, 1999**

[54] **APPARATUS FOR GENERATING ODOR UPON ELECTRONIC SIGNAL DEMAND**

[75] Inventors: **Firooz Rasouli**, Midlothian, Va.; **Hamid Arastoopour**, Downers Grove; **Ali Oskoule**, Chicago, both of Ill.

[73] Assignee: **Illinois Institute of Technology**, Chicago, Ill.

[21] Appl. No.: **08/907,230**

[22] Filed: **Aug. 6, 1997**

Related U.S. Application Data

[60] Provisional application No. 60/023,465, Aug. 6, 1996.

[51] **Int. Cl.**[6] **A61L 9/00**

[52] **U.S. Cl.** **422/124**; 422/123; 422/125; 422/305; 422/306; 239/57; 239/60; 392/386; 392/390

[58] **Field of Search** 422/4, 5, 22, 120, 422/122, 123, 124, 125, 305, 306; 239/57, 60; 392/386, 390

[56] **References Cited**

U.S. PATENT DOCUMENTS

2,562,959	8/1951	Stern .	
2,871,526	2/1959	Bulloff	21/108
4,009,384	2/1977	Holland .	
4,037,352	7/1977	Hennart et al.	43/129
4,556,539	12/1985	Spector	422/5
4,603,030	7/1986	McCarthy	422/4
4,604,114	8/1986	Ward	55/279
4,905,112	2/1990	Rhodes	422/124
5,023,020	6/1991	Machida et al.	422/124
5,069,876	12/1991	Oshinsky	422/4
5,069,877	12/1991	Pozzo	422/4
5,178,839	1/1993	Spector	422/123
5,217,696	6/1993	Wolverton et al.	422/121
5,273,690	12/1993	McDowell	422/124
5,424,049	6/1995	Giolitti et al.	422/305
5,565,148	10/1996	Pendergrass	422/124
5,574,821	11/1996	Babasade	392/392
5,591,409	1/1997	Watkins	422/110
5,734,590	3/1998	Tebbe	364/514 A

FOREIGN PATENT DOCUMENTS

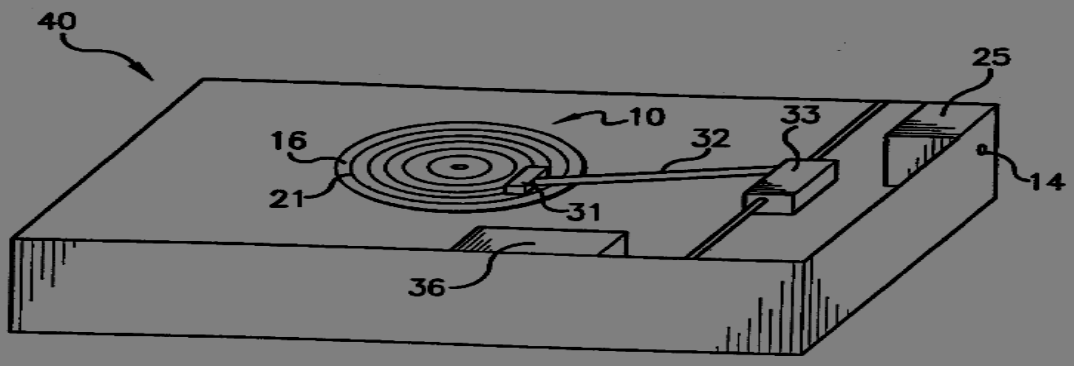
0123746	7/1984	European Pat. Off. .
0238983	9/1987	European Pat. Off. .
2501468	9/1982	France .
2279010	12/1994	United Kingdom .

Primary Examiner—Robert J. Warden, Sr.
Assistant Examiner—Fariborz Moazzam
Attorney, Agent, or Firm—Pauley Petersen Kinne & Fejer

[57] **ABSTRACT**

An apparatus for generating odor upon electronic signal demand using a disk having an aroma-impregnated adsorbent and a substrate. The disk is inserted into a disk drive that receives signals from a user and/or a server computer. A controller within the disk drive supplies an electric, mechanical or thermal signal to the disk, resulting in the heating of the adsorbent. The controller may also activate a blower to distribute the scent produced by the heated adsorbent and to cool the adsorbent at the end of the scent distribution cycle.

21 Claims, 3 Drawing Sheets



US 20030164557A1

(19) **United States**

(12) **Patent Application Publication** (10) **Pub. No.: US 2003/0164557 A1**

Chung et al. (43) **Pub. Date: Sep. 4, 2003**

(54) **INTERACTIVE, AUTOMATED AROMA DIFFUSER WITH INTERFACE TO EXTERNAL DEVICE**

(76) Inventors: **Caleb Chung**, Boise, ID (US); **Gary Schwartz**, Boise, ID (US)

Correspondence Address:
PEDERSEN & COMPANY, PLLC
P.O. BOX 2666
BOISE, ID 83701 (US)

(21) Appl. No.: **10/351,100**

(22) Filed: **Jan. 22, 2003**

Related U.S. Application Data

(60) Provisional application No. 60/351,454, filed on Jan. 22, 2002.

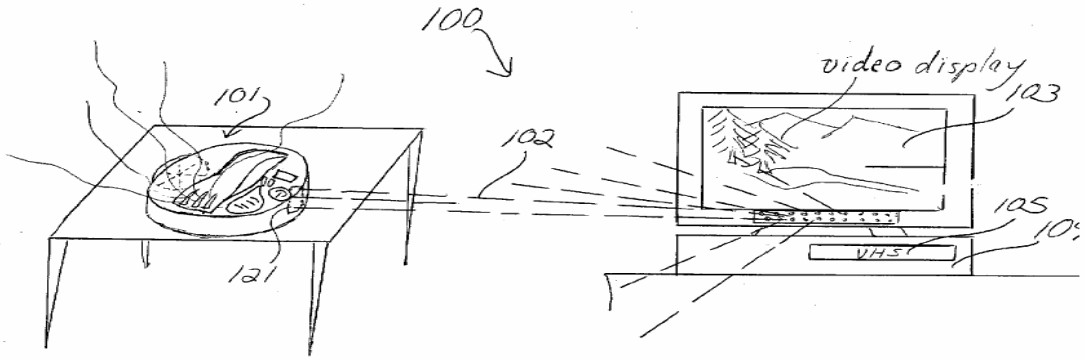
Publication Classification

(51) **Int. Cl.**[7] **B01F 3/04**

(52) **U.S. Cl.** **261/26**; 261/DIG. 8444576

(57) **ABSTRACT**

An aroma diffuser that may be adapted to cooperate with a computer, television, CD player, or other media device that is separate and external to the diffuser, to emit one or more aromas into a room or space upon a signal from said external device. The signal from the external device may be wired or wireless, but preferably is a wireless, audible signal included in the CD, VHS, or other pre-recorded media. This way, the control signal is produced by playing of the media on a commercially-available external device, such as any television, without modification of said device's hardware or firmware. Optionally, the diffuser may be manually controlled, or may have multiple modes so it can be manually controlled by the user, or controlled through the user's PC, audio player, or television/VCR unit. The diffuser system may direct/connect the user an internet website for purchase of scent products or other accessories for the system.



US006524537B1

(12) **United States Patent**
Lee

(10) **Patent No.: US 6,524,537 B1**
(45) **Date of Patent: Feb. 25, 2003**

(54) **FRAGRANCE EMITTER FOR USE WITH INTERNET**

(76) Inventor: **Chum Lee**, No. 39-5, Gau Gaung Road, Yung-He, Taipei (TW)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/519,685**

(22) Filed: **Mar. 7, 2000**

(30) **Foreign Application Priority Data**

Aug. 4, 1999 (TW) ..... 088213100 U

(51) **Int. Cl.**[7] **A62B 7/08**
(52) **U.S. Cl.** ..... **422/124**; 364/502; 364/509; 364/514 A; 422/108; 422/116; 422/119; 422/120; 422/123
(58) **Field of Search** ..... 422/1, 4, 5, 108, 422/116, 119, 120, 123, 124; 364/502, 509, 514 A

(56) **References Cited**

U.S. PATENT DOCUMENTS

5,114,625 A * 5/1992 Gibson 261/102
5,174,967 A * 12/1992 Fukuhara 261/65
5,565,148 A * 10/1996 Pendergrass, Jr. 261/30
5,591,409 A * 1/1997 Watkins 422/1
5,724,256 A * 3/1998 Lee et al. 422/105
5,734,590 A * 3/1998 Tebbe 700/94
5,924,597 A * 7/1999 Lynn 222/1
5,972,290 A * 10/1999 De Sousa 422/123
6,053,738 A * 4/2000 Ivey, Jr. 273/460

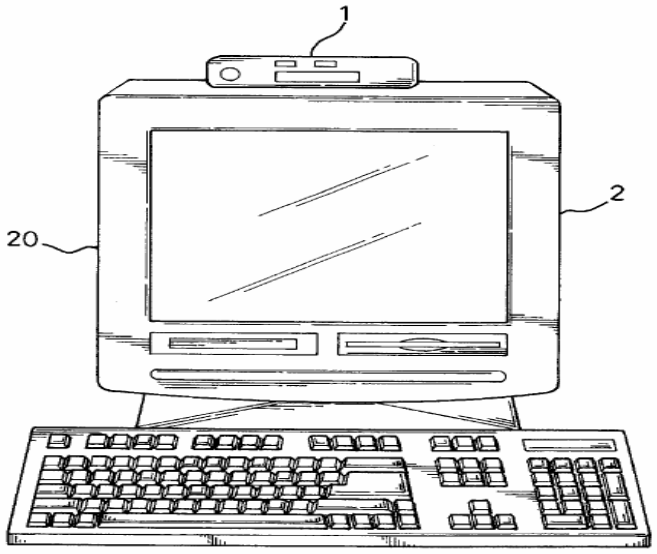
* cited by examiner

Primary Examiner—Krisanne Thornton
(74) *Attorney, Agent, or Firm*—Ostrolenk, Faber, Gerb & Soffen, LLP

(57) **ABSTRACT**

A fragrance emitter used with internet is disclosed. The fragrance emitter is able to emit various kinds of fragrance stored in vessels according to the command sent by a frequency detector which is used to search for the existence of a specific frequency specially used by a specific web site. Therefore, when the existence of a specific frequency matches with a predetermined frequency, the electromagnetic valve is able to activate the movement of a valve mounted on a fragrance vessel in an air tight manner, such that the fragrance is ventilated and mix with the air by a fan.

4 Claims, 5 Drawing Sheets



APPENDIX E: DECLASSIFIED MILITARY ABSTRACTS

Chemical, Biological, and Nuclear Terrorism/Warfare: A Bibliography

Chemical: Technical Reports

*Although there are a number of very relevant reports issued with distribution limitations (e.g. FOUO or DOD only) due to the public nature of this bibliography, this section includes unclassified/unlimited distribution references only. Abstracts were taken from various databases and were written by the authors of the documents cited or by the abstracting service from which the citations were generated not by the author of this bibliography (*http://www.nps.edu/library/).

Anderson, Donnie P. **Army's Commitment to Supporting the Homeland Security Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Weapon Terrorist Threat: Can the Reserve Components Meet the Requirement by Themselves?** Carlisle Barracks, PA: Army War College, 10 April 2001. 30p.

Abstract: The United States Government has identified of highest priority the development of effective capabilities for preventing and managing the consequences of terrorists use of chemical, biological, radiological, nuclear and high-yield explosive (CBRNE) materials and weapons on the American homeland. The Department of Defense (DOD) and Army both have a significant role in this effort. This paper will look at those roles and focus on the Army's ability to support the Homeland Security (HLS) CBRNE terrorist threat in the areas of agent sampling, detection, identification, and decontamination operations. Specifically, it will address the Reserve Components (RC) capability for responding to an incident and demonstrate the value-added of Active Component (AC) forces. The conclusion is the RC cannot fulfill the Department of the Army's commitment to this important mission by itself: AC forces must assume a more prominent role to ensure an adequate DOD response in this critical area.
http://handle.dtic.mil/100.2/ADA388953
Accession Number: ADA388953

Anderson, William. **Bugs & Drugs: Chemi-Bio Terrorism & the U.S. Government**. Quantico, VA: Marine Corps Combat Development Command, May 2002. 59p.

Abstract: The U.S. Public is capable of assimilating the facts regarding the threat of chemical and biological terrorism; however, the United States Government (USG) has failed to systematically inform its populace about this threat to their security.
Accession Number: ADA407502

Arca, Victor J., *et al.* **Chemical Protective Clothing For Law Enforcement Patrol Officers and Emergency Medical Services When Responding to Terrorism With Chemical Weapons**. Aberdeen Proving Ground, MD: Edgewood Chemical Biological Center, January 2001. 27p.

Abstract: This report covers Man In Simulant Testing (MIST) of the following commercially available, Level C chemical protective suits: the Tyvec(trade name) Protective Wear(trade mark) suit (garage-type, for mechanics), the Kappler CPF(trade name) suit (model # 4T434), the TyChem(trade name) 9400 (style 94160) suit, the TyChem(trade name) SL (style 72150) suit, and the Tyvec (trade name) ProTech F suit. These suits are being considered by law enforcement agencies for use at scenes where chemical warfare agents have been used by terrorists. This testing examined how well the complete protective suit ensembles protect the wearer against vapor adsorption by the skin by exposing test participants wearing the suits to a chemical agent simulant (methyl salicylate) and measuring the Physiological Protective Dosage Factor (PPDF) the wearers received while performing a set of typical law enforcement activities. The results showed that the respective suits provided the wearers with the following average Overall PPDF: standard police uniform - 2.0; Tyvec(trade name) - 4.0; CPF(trade name) 4 - 17.6; TyChem(trade name) 9400- 16.5; TyChem(trade name) SL - 23.7; and the Tyvec(trade name) ProTech F - 41.8.

http://handle.dtic.mil/100.2/ADA387092
Accession Number: ADA387092

Bagley, R. W., Jr. **Responding to Chemical Attack**. Newport, RI: Naval War College, Department of Operations, February 1991. 23p.

Abstract: Responding to chemical attack. In view of Iraq's stated intention of using chemical weapons in the Persian Gulf War, the Coalition forces must be prepared to respond. Iraq is capable of conducting such an attack. While the use of chemical weapons may not be militarily significant, the political effect of the use and the response to it may be very significant. Responses including the use of chemical and nuclear weapons are assessed in terms of their legality, political cost, and military effectiveness and found unacceptable. Reliance on diplomatic protests and on post-war criminal sanctions are judged ineffective. A response in the form of increased conventional attack on the Iraqi chemical infrastructure is recommended because that response will preserve the present Coalition, effectively counter the chemical attack, contribute to regional stability, and enhance the reputation of the United States for lawfulness and dependability.

Accession Number: ADA236609

Battaglia, Deboral A., David W. Klinger and Erica L. Rall. **Developing a Rapid Situation Awareness: Understanding the Challenges Faced by First Responders to Biological and Chemical Events**. Fairborn, OH: Klein Associates, Inc., July 2002. 28p.

Abstract: Since the terrorist attacks on September 11, 2001, the threat of a biological or chemical terrorist attack on our society has transformed from a distant unease to a major, looming concern. National, state and local organizations are trying to prepare themselves for a threat that is of terrifying consequences and yet ambiguous in how or if it will even present. This effort aimed to understand the cognitive demands faced by first responders to biological and chemical terrorist events. Data collection involved employing Cognitive Task Analysis (CTA) interviews with officials at the local and federal level, attending a conference outlining major research advances in this area, and collecting observations at regional bioterrorism exercises. This report describes the findings using the Advanced Team Decision Making model (Zsambok, Klein, Kyne and Klinger, 1992) as a framework for understanding the challenges teams face in rapidly building and developing their situational understanding in response to these events. The findings from this study are important leverage points for understanding current gaps in response preparedness and areas for future research and development.

http://handle.dtic.mil/100.2/ADA408914
Accession Number: ADA408914

Besosa, Miguel A. **Role of the National Guard in Responding to Weapons of Mass Destruction (WMD) Attacks in the U.S.: Where Do We Stand**. Maxwell Air Force Base, AL: Air University, Air Command and Staff College, April 2001. 58p.

Abstract: The potential for terrorists' use of weapons of mass destruction (WMD) threatens Americans every day To many nations and groups, their only means to counter the United States (U.S.) is with nuclear, biological, or chemical weapons According to most experts, terrorists use of WMD is no longer a question of 'if' they will be used, but 'when.' When domestic capabilities were found to be lacking in this regard, Congress enacted legislation, Public Law 104-201, and named the National Guard as the primary responder to domestic WMD events. It is evident gaps and shortfalls remain in the National Guard's (NG) ability to respond to domestic WMD attacks, The purpose of this paper is to examine the critical gaps and shortfalls encountered by the CSTs since their activation, This is done by investigating any available materials concerning the NG involvement in the program, identifying the critical gaps and shortfalls encountered by the CSTs, and to coming up with recommendations to correct them. This paper examines current U.S. policy and strategy to counter terrorist uses of weapons of mass destruction. The second section will examine the CSTs infrastructure, the third section identifies and discusses the predominant gaps and shortfalls encounter by the teams. The final section details current shortfalls and recommendations to improve the overall CST capability.
http://handle.dtic.mil/100.2/ADA407098
Accession Number: ADA407098

Bester, William T. **New Enemy: Silent, Lethal, and Invisible**. Carlisle Barracks, PA: Army War College, April 1998. 44p.

Abstract: The possibility of a terrorist attack on the United States, utilizing a weapon of mass destruction (WMD) has increased significantly over the past decade. This paper analyzes the effects of a terrorist attack on the United States using a WMD with a biological agent. The paper addresses six major areas. First, it examines the feasibility of such an act. Second, it reviews health-related implications. Third, it examines the economic effects of such an occurrence in a large metropolitan area. Fourth, it identifies the response requirements needed to react to such a catastrophe. Fifth, it looks at the impact on civil structure and order. Finally, it identifies resources currently available to respond to a WMD attack and provides recommendations for systems still needing development and implementation in order to respond appropriately and effectively to this kind of terrorist activity.
Accession Number: ADA346005

Birdsong, George M. **Weapons of Mass Destruction -- Terrorist Use and the State of Domestic Response**. Carlisle Barracks, PA: Army War College, March 1997. 25p.

Abstract: United States Military Forces continue to refine and modernize their capability to react to and operate in the presence of weapons of mass destruction (WMD), including nuclear, chemical, and biological weapons. While this threat remains substantial, effectively dealing with it on the modern battlefield remains problematic. On the contrary, the WMD threat to domestic population centers and their infrastructure is growing at an alarming rate. Furthermore, the ability of local governments and emergency responders to effectively deal with almost any use of nuclear, chemical, or biological weapons is virtually non-existent. This paper examines the menace of domestic WMD use and the resources available to recover from their use. Analysis concludes that the government, in particular the Department of Defense, should play a larger role in preparing state and city authorities for possible WMD use and recovery.
Accession Number: ADA327426

Blueprint For the National Domestic Preparedness Office. Washington, DC: National Domestic Preparedness Office, 2001. 42p.

Abstract: Success in preventing, preparing for and responding to a terrorist attack in the United States involving conventional or non-conventional weapons of mass destruction (WMD) will depend upon the establishment and maintenance of a coordinated crisis and consequence management infrastructure. Emergency responders who arrive first on the scene, as well as those in the medical profession who provide interim treatment, must be adequately trained, equipped, and exercised to ensure their ability to effectively respond and conduct relief and recovery operations as part of a multi-agency team. The federal agencies recognize that the response to bioterrorism will be qualitatively different from a chemical event and will primarily involve the public health and medical communities. Events within the United States and against Americans abroad have demonstrated the need to enhance the nation's domestic preparedness activities. The United States Congress and the President have recognized the need for federal programs to assist state and local jurisdictions in preparing for the threat of WMD terrorism.
http://www.securitymanagement.com/library/ndpo1201.pdf
Accession Number: PB2001104993

Bray, Gary D. **Countering Terrorist Use of Weapons of Mass Destruction: A Future Role For the National Guard**. Carlisle Barracks, PA: Army War College, March 1998. 43p.

Abstract: This project defines the terrorist threat to use weapons of mass destruction in the United States. Several chemical and biological agents that could be used in the attack are described. Current statutes are researched to insure the legality of using the military in combating terrorism here in the United States. An examination of current legislation and security strategies reveals the growing concern senior leadership feels toward this issue. Finally, the National Defense Panel recommendations using the National Guard and Army Reserve in consequence management are analyzed. The analysis confirms the appropriate element of the military to perform this mission should be the National Guard.
Accession Number: ADA346389

Broadwater, Jeffery D. **High Resolution Modeling of a Terrorist Chemical Attack in an Urban Area**. Monterey, CA: Naval Postgraduate School, June 1999. 112p.

Abstract: This thesis demonstrates the use of Janus in Modeling Military Operations Other Than War, MOOTW. Janus has many uses throughout the United States military. Lately, MOOTW have become a major percentage of the U.S. military's efforts. Using Janus to model these operations can help predict casualties, determine if new pieces of equipment make a difference in the operation, and help evaluate "what ifs" in operations. More importantly, conducting a simulation before carrying out an actual exercise saves money and people's time and effort. The threat of a terrorist chemical attack is a very likely event in this day and age as demonstrated by the 1995 chemical attack in a Japanese subway. Current U.S. policy has allocated certain resources to assist local governments in the event of an emergency. Unfortunately, these assets can not immediately respond to a chemical crisis. Time waiting for these assets to arrive must be spent wisely to save lives. Local governments do not all have the same capabilities available to respond to a chemical attack. Using a high resolution combat model such as Janus at the local level will help determine assets that will save lives and money.
http://handle.dtic.mil/100.2/ADA365438
Accession Number: ADA365438

Brown, Michael T. **Terrorist Use of Weapons of Mass Destruction Within the United States: Asymmetric Warfare Paradigm in the 21st Century**. Carlisle Barracks, PA: Army War College, Strategic Studies Institute, March 1997. 33p.

Abstract: The use of Weapons of Mass Destruction (WMD) by terrorists within the United States presents a clear and present danger to national security. In virtually every region of the world, nation

states are arming themselves with WMD. Coupled to the rising spread of WMD is the growing list of nations sponsoring worldwide terrorism. The proliferating nature of this combined threat of WMD and terrorism is changing the paradigm of asymmetrical warfare as we approach the new millennium. Reviewing the U.S. Government responses to terrorism and WMD reveals a fragmented framework that addresses these threats separately, without one federal agency in the lead. The world witnessed this new paradigm of asymmetrical attack when the Japanese religious cult, Aum Shinrikyo or Supreme Truth, attacked the Tokyo subway system using the chemical nerve agent Sarin on 20 March 1995. The Department of Defense should take action and assign this critical mission to a Joint WMD response force to support the federal, state and local crisis response framework.
http://handle.dtic.mil/100.2/ADA326609
Accession Number: ADA326609

Cain, Eddie and Mark W. Walsh. **The Chemical Weapons Convention: Will it Assure The End of Chemical Warfare?** Carlisle Barracks, PA: Army War College, February 1993. 48p.

Abstract: After more than a generation of negotiations, the Conference on Disarmament (CD) has completed a draft treaty banning the development, production, stockpiling, transfer, and use of chemical weapons (CW). Unfortunately, despite all the successful work put into the CWC it will not, and cannot assure a permanent halt to chemical warfare. This paper analyzes the merits of having a CWC treaty to thwart chemical weapons proliferation. It will offer a way to strengthen the verification regime. Finally, from this analysis, the paper reaches conclusions concerning what CW policy best supports U.S. national interests.
Accession Number: ADA263851

Campbell, James K. **Weapons of Mass Destruction and Terrorism: Proliferation by Non-State Actors**. Monterey, CA: Naval Postgraduate School, December 1996. 354p.

Abstract: Executive Order No. 1298 signed by President Clinton on November 14, 1994 declared a national emergency with respect to the unusual and extraordinary threat that proliferation of weapons of mass destruction (those weapons categorized as nuclear, chemical or biological) poses to the national security, foreign policy, and economy of the United States. In the wake of the Cold War, a new world disorder seems to be emerging wherein the legitimacy of many states is being challenged from within by increasing non-state calls for self determination from the likes of religious cults, hate groups, isolationist movements, ethnic groups, and revivalist movements. These movements often prey on the insecurities of the population, offering to fill psychological, social, political, or religious security needs of those who would join them. Religious oriented groups appear to share a common ideology which rejects existing social, economic, and political structure demanding a drastic revision of the world - a world where they become the authoritarian, dominant influence. These are the Post-Modern Terrorists who possess a ripeness to threaten use of weapons of mass destruction. This study presents an argument suggesting that terrorist groups operating under the veneer of religion are truly the most likely candidates to threaten use of mass destruction in a mass casualty causing terrorist act.
http://handle.dtic.mil/100.2/ADA323947
Accession Number: ADA 323947

Carter, Robert D. **Domestic Terrorism and Our National Security Strategy**. Carlisle Barracks, PA: Army War College, April 1998. 37p.

Abstract: The threat of terrorism has encroached our national borders and has created a heightened sense of vulnerability among many Americans. President Clinton has stated, Fighting terrorism is and will for a long time to come be one of the top priorities of the United States. Two acts passed in 1996 have strengthened our fight against terrorism, the Antiterrorism and Effective Death Penalty Act and the Defense Against Weapons of Mass Destruction (WMD) Act. The Defense Against WMD Act designated the Department of Defense the executive agent for coordination of assistance in responding to threats involving biological and chemical weapons. The focus of this research project will be to follow this trail and analyze DOD's course of action in meeting their obligation and assess the probability that DOD will maintain this function after the 1 October 1999 legislative mandate.

http://handle.dtic.mil/100.2/ADA341465
Accession Number: ADA341465

Chemical, Biological, Radiological and Nuclear Terrorism: The Threat According to the Current Unclassified Literature. Washington, DC: National Defense University, May 2002.47p.

Abstract: The prospect of chemical, biological, radiological, and/or nuclear (CBRN) terrorism is recognized by the United States government as an acute security challenge, Particularly following the tragedy of September 11, 2001, but also for several years prior, senior U.S. officials and official government reports have underscored the likelihood, over time, of terrorist organizations coming into possession of such unconventional materials, and the prospect of their use against the United States homeland, U.S. forward-deployed forces, or U.S. friends and allies, Toward the end of the last century, this concern was heightened, among other events, by the Japanese cult Aum Shinrikyo's 1995 use of sarin in the Tokyo subway The combination of increasing availability of technology and expertise, a perceived mass-casualty motive structure for particular terrorist organizations, the impending end of a millennium, a spate of conventional attacks against U%S assets - World Trade Center, 1993; Oklahoma City Federal Building, 1995; American embassies in Tanzania and Kenya, 1998; and the U.S.S. Cole, 2000 - and both the widespread suspicion of terrorists seeking CBRN weapons and the actual sub-national employment of a chemical agent all contributed to this general assessment, More recently, the prospective linkage between terrorist organizations and state actors with weapons of mass destruction programs has become an acute security concern. Indeed, this nexus is central to the logic of the emergent 'Bush Doctrine'. As Secretary of Defense Donald Rumsfeld testified in May 2002, 'we have to recognize that terrorist networks have relationships with terrorist states that have weapons of mass destruction, and that they inevitably are going to get their hands on them, and they would not hesitate one minute in using them. That's the world we live in'.

http://handle.dtic.mil/100.2/ADA404213
Accession Number: ADA404213

Cooper, Peter C. **Chemical/Biological Weapons Taboo: Is There Relevance For Today**. Carlisle Barracks, PA: Army War College, April 2000. 27p.

Abstract: The President of the United States has declared a national emergency to deal with the potential specter of a chemical or biological attack against Americans, yet chemical and biological weapons have been used infrequently throughout history compared to conventional weapons. Leonard A. Cole in an article in the Scientific American uses the term 'poison taboo' to describe the abhorrence mankind feels toward biological weapons. The use of the word taboo is interesting and, according to Webster, implies something 'forbidden to profane use... because of supposedly dangerous supernatural powers'. Throughout the ages, man has given biological and chemical weapons supernatural status, partly because of their nature. Does this help explain this apparent dichotomy between our fear and the lack of their use. Are chemical and biological weapons sufficiently morally repugnant today to inhibit their use in a world accustomed to graphic violence. Or, are they just becoming another tool in national arsenals and terrorist caches to be used to offset the awesome power of the United States. The answers to these questions have dramatic consequences for the security of our nation and present remarkable challenges as well as windows of opportunity. This essay explores the relevance of the poison taboo to the security of the United States today by looking at its historical development, at the mechanisms of terrorist restraint in the use of CB weapons, and at a blueprint for a national rhetoric to enhance its deterrent value.
Accession Number: ADA378219

Davis, Edwin F., Jr. **Counterterrorism: A National Security Priority For the 21st Century**. Carlisle Barracks, PA: Army War College, April 1997. 36p.

Abstract: As the 20th century draws to a close, the United States has emerged as the world's only superpower. International terrorism is increasing. No other country possesses the wherewithal to

feasible for military assets to support the Lead Federal Agency while remaining ready to fight and win the nations wars.
http://handle.dtic.mil/100.2/ADA406640
Accession Number: ADA406640

Dickinson, Lansing E. **Military Role in Countering Terrorist Use of Weapons of Mass Destruction**. Maxwell Air Force Base, AL: Air University, Air War College, April 1999. 74p.

Abstract: Terrorist use of weapons of mass destruction threatens Americans and our armed forces every day. To many nations and groups, their only means to counter the United States is with nuclear, biological, or chemical weapons. The terrorist use of weapons of mass destruction is no longer a question of "if" they will be used, but a question of "when" they will be used. This paper looks at the US military capability to counter terrorist use of weapons of mass destruction. It describes the terrorist threat to US forces and motives and reasons terrorists would use these types of weapons. Our current national policy, strategy and doctrine highlight the problem, but show a need to improve interagency coordination and cooperation. On the military level, combating the threat is an integral part of our strategy but needs increased emphasis at the planning level. Capabilities exist to deter or counter the threat; protect our forces; and sustain and operate after an NBC attack. But countering a terrorist threat presents unique challenges to future leaders and requires improvements in intelligence, equipment, training and education.
http://handle.dtic.mil/100.2/ADA395120
(**Accession Number: ADA395120).**

Drake, Gordon, Warrick Paddon, and Daniel Ciechanowski. **Can We Deter Terrorists From Employing Weapons of Mass Destruction on the U.S. Homeland?** Carlisle Barracks, PA: Army War College, April 2003. 84p.

Abstract: Information discovered as a result of the current war on terrorism suggests a terrorist-led attack on the U.S. homeland involving weapons of mass destruction (WMD) remains a very real possibility. Some believe the U.S. faces its greatest WMD threat since the 1962 Cuban Missile Crisis, but many discount the effect deterrence can have on terrorist groups. Deterrence, however, is an attractive option in the costs to implement a deterrence-based strategy are minimal when compared to defending the entire homeland or defeating all elements of a threatening terrorist organization. Little research, however, has been done to evaluate the effectiveness deterrence can have on a group bent on harming the U.S. with WMD.
Accession Number: ADA415856

Torrens, Linda E. **Conflict in the 21st Century: Counterstrategies For the WMD Terrorist. Maxwell Air Force Base, AL: Air University**, April 1999. 53p.

Abstract: For years, the US military has prepared to fight against opponents armed with nuclear, biological, and chemical capabilities. These weapons of mass destruction (WMD) in the hands of traditional, state actors have been at the forefront of US defense planning. The end of the Cold War and the demise of the Soviet Union have allowed us to focus on new threats to US security. WMD terrorism will play a larger role in this new uncertain security environment for several reasons. First, transnational threats are no longer kept in check by a bipolar world. Secondly, terrorists may have greater access to WMD materials today than ever before. And thirdly, the information revolution has made not only weaponization knowledge freely available, but has also improved the organizational capabilities of diverse terrorist groups. This paper examines the WMD terrorist threat and addresses counterstrategies for reducing the risk. Conclusions include a need for heightened awareness of the threat. Recommendations include strengthening domestic and international controls and legal structures regarding WMD materials, using diplomatic pressure and economic means to deter or reduce the likelihood of WMD terrorism, and improving defensive and responsive capabilities.
http://handle.dtic.mil/100.2/ADA395718
Accession Number: ADA395718

Grabow, Chad Lee. **Implications and Effects of Advanced Biological and Biological/Chemical Weapons at the Operational Planning Level**. Final Report. Newport, RI: Naval War College, Department of Operations, 21 June 1991. 33p.

Abstract: This paper analyzes recent research and advances in biological and biological/chemical technology. It examines the imposing threat and significance to the Biological Weapons Convention of 1972. It then discusses how biological and biological/chemical weapons effects the operational level and operational planning. This paper offers projections, opinion on deficiencies/risk, and suggests alternatives. Finally, conclusions are presented offering challenges and concerns.
Accession Number: ADA240460

Erichsen, Sven C. **National Guard Weapons of Mass Destruction Civil Support Teams: Performing as Required?** Fort Leavenworth, KS: Army Command and Staff College, School of Advanced Military Studies, May 2002. 62p.

Abstract: The Department of Defense is also in the process of reevaluating its contribution to homeland security in the aftermath of the September 11 attacks. Of particular concern is the DoD plan for assisting civilian authorities in consequence management - the measures taken to protect public health, safety, and the environment, to restore essential government services, and to provide emergency relief to governments businesses and individuals affected by the consequences of terrorism. A significant DoD contribution to the consequence management aspect of homeland security has been the development of the National Guard Weapons of Mass Destruction - Civil Support Team (WMD-CST), a new type of unit designed to provide civilian authorities military support in response to WMD attacks involving the use of nuclear, biological, chemical, or radiological (NBCR) weapons. The development of the WMD-CST concept has raised considerable debate over the merits of the new organization. Previous authors argued that the WMD-CST is incapable of providing timely support to local authorities. Others take the criticism of the WMD-CST a step further, calling into question the ability of the Department of Defense to provide personnel sufficiently trained to provide meaningful support to civilian first responders. Positive reviews emphasized the WMD-CSTs' ability to respond rapidly to events, because of their ability to operate under Title 32 or Title 10 authority.
http://handle.dtic.mil/100.2/ADA403167
Accession Number: ADA403167

Webb, Danny W. **The Prospects For International Terrorist Groups Employing Chemical Weapons**. Maxwell Air Force Base, AL: Air University, Air War College, April 1999. 59p.

Abstract: There has been much discussion and debate among security analysts, scholars, and politicians about the possible use of weapons of mass destruction. This paper examines the prospects for international terrorist groups employing chemical weapons. Specifically, it argues that terrorists have the capabilities to employ chemical weapons but will be constrained from using them. A thorough search of available open literature material from books, periodicals, and the internet was conducted to compile the facts of this paper. Limited discussion with terrorist experts on the Air War College staff and the Defense Threat Reduction Agency were also incorporated into this paper. With the exception of the Aum Shinrikyo, there is no open literature support for terrorist possession of a chemical weapon. Empirical evidence does support their ability to buy, steal, or build their own chemical weapon capability. Political, ideological and moral constraints preclude the traditional terrorist employment of a chemical weapon. However, there is a growing faction of terrorists, the religious radicals, who show a proclivity to use chemical weapons to further their cause. The United States has developed cogent policies and procedures to deter, detect and respond to the chemical weapon threat. Additionally, programs have been instituted to train first responders in all major American cities. In concluding, the paper recognizes that traditional terrorists are constrained from using chemical weapons but the religious radical is not.
http://handle.dtic.mil/100.2/ADA395721
Accession Number: ADA395721

Wilcox, David L. **Domestic Preparedness and the WMD Paradigm**. Fort Leavenworth, KS: Army Command and Staff College, School of Advanced Military Studies, May 1998. 67p.

Abstract: The threat or use of chemical or biological weapons is a likely condition of future warfare-including the early stages of war, to disrupt operations and logistics. That threat, whether perceived or real, has haunted U. S. military leaders and planners in every conflict since WWI. Now that threat has reached the shores of the United States. For many years, terrorist acts aimed at US citizens or interests were conducted outside of American borders. The geneses of modern terrorism in the U.S. were the bombing incidents of the New York World Trade Center and the Federal Building in Oklahoma. These bombing incidents were the largest terrorist attacks ever conducted in the continental U.S. These bombings demonstrated the real and deadly threat of terrorism to America. This monograph examines the U.S. domestic preparedness program as it relates to chemical and biological weapons. By investigating the terrorist threat, proliferation of weapons of mass destruction and the domestic preparedness program, it will show that the U.S. has demonstrated the 'will' and need for such a program but still lacks resolve to fully implement what resources are required.
Accession Number: ADA357324

Ward, Judith. **Homeland Defense: Are We There Yet?** Maxwell Air Force Base, AL: Air University, April 2001.

Abstract: The threat of a catastrophe from terrorist's use of a biological weapon is increasing in probability in light of events such as the 1995 sarin nerve gas attack on the Tokyo subway, disclosure regarding the former Soviet Union's sophisticated bioweapons program, and discoveries of Iraq's large-scale efforts to produce and weaponize biological agents, public awareness about terrorism as certainly heightened during the Y2K alerts and the arrest of Algerians linked to Osama bin Laden at the United States-Canadian border, but also may be a result of increasingly public awareness through books, such The Cobra Event and Biohazard programs, such as ABC's "Biowar". http://handle.dtic.mil/100.2/ADA406250
Accession Number: ADA406250

Walk, Robert D. **The Chemical Corps and Homeland Security**. Carlisle Barracks, PA: Army War College, April 2003. 42p.

Abstract: Homeland security is the number one priority in the draft National Military Strategy released in September 2002. The US Army Chemical Corps has, in its recent history, focused on supporting the Army's overseas force projection mission. All equipment, doctrine and training is developed and fielded for this mission. With the advent of terrorism in the United States, there have been on- going discussions on refocusing the mission to include the homeland security mission. Technology and regulations have changed the civil response landscape since the Chemical Corps was last involved in the 1960's. Responders in the US now must fulfill a bewildering array of required training and equipment certifications before they can legally respond in the US. This paper examines the historical Chemical Corps mission and the homeland defense mission (to include Posse Comitatus). It also examines the Chemical Corps through elements of the Army Force Management requirements generating process (Doctrine, Organizations, Training and Materiel) to determine whether the homeland security mission can be feasibly supported by the Army Chemical Corps. A discussion of what the Chemical Corps would do in Homeland Security operations is also included. Finally, recommendations on changes to Chemical Corps' doctrine, training and missions are included.
Accession Number: ADA415740

APPENDIX F: YESTERDAY'S DIRTY UNMANNED AIR VEHICLES (UAVS)

[Documents available through Los Alamos Labs unclassified/declassified records]

[redacted] UNCLASSIFIED

FINAL DETERMINATION
UNCLASSIFIED
L. M. Redman
JAN 23 81

2 3 2 A

J. R. Oppenheimer
I. I. Rabi
20 April 1944 J. Chadwick

Subject: Possible Use of Radioactive Poison in Rocket Propelled, Unmanned Aircraft.

MEMORANDUM to Major General L. R. Groves.

1. During my last visit to Washington on 14 March 1944, I was accompanied by Major Furman to the Pentagon and there shown the present information on rocket installations and additional unknown construction on the sector in France between 100 and 150 miles from London and Bristol. It appeared that fairly definite information is available on the launching stations but very little is available on the seven to ten larger stations, and these are guarded with great energy.

2. At the time I could form no opinion as to the possible nature of the contemplated material except that it must be a very "hot" chemical since the installations were literally under the guns and bombs of the enemy, the opposite place where a delicate chemical job should be performed. from that in which.

3. Recently, I have discussed with Rotblat, one of Chadwick's men, the work done by Chadwick's group in England in connection with investigating the possibilities of radioactive poisons evolved from disintegration products of a pile. I understand that such a pile would not be extremely difficult to set up and operate and that it could be "milked" every three days. It would then be necessary to separate the radioactive materials and transport these behind very heavy lead armor to the launching point.

4. The combination of an apparent plan to use unmanned aircraft and the possibility that some form of complicated installation is being built in locations which might serve as feeders to the launching point, suggests the possibility that the "hot chemical" might be radioactive disintegration products which the Germans considered so "hot" that they could not transport them from manufacturing points in Germany by any available transportation. These might be placed in bombs with ordinary explosives to be functioned over the ground to gain maximum distribution of the radioactive products. It is unnecessary to picture the destructive possibilities of such an arrangement.

5.

CLASSIFICATION CANCELLED
PER DOC REVIEW JAN. 1973
OK J.&W. 4/17/79

[redacted] UNCLASSIFIED

[redacted] UNCLASSIFIED

5. Essentials in the construction of a scheme such as outlined above would be:

a. Some material for lining a pile. This might be heavy water or blocks of graphite. Other possibilities exist.

b. Uranium for use in the pile. This might be in some liquid solution.

c. Heavy walls surrounding pile. It might be located in the ground.

d. A small chemical plant for separating the radioactive products. This would require heavy lead for protection of personnel.

e. During actual operation or rehearsal operation, blood counts would probably be taken of operating personnel.

f. Final loading and launching positions would probably be done behind heavy lead or very thick concrete protection.

W. S. PARSONS,
Captain, U.S.N.

NR 210 17 13

OK J.F.W 4/17/75
CLASSIFICATION CANCELLED
PER DOC REVIEW JAN. 1973

[redacted] UNCLASSIFIED

The intention to use the latest vehicle to launch a biochemical attack is traceable. This document illustrates how far forward-thinking took certain scientists and intelligence officers (since the late 1930's) in their respective roles as engineers and investigators [to come up with scientific breakthroughs and anticipate (uncover) the most dreadful threats].

Information

LOCKHEED MARTIN TO DESIGN NANO AIR VEHICLE TO MONITOR THE URBAN BATTLEFIELD

CHERRY HILL, NJ, July 20, 2006—The Defense Advanced Research Projects Agency (DARPA) awarded Lockheed Martin (NYSE:LMT) a $1.7-million, 10-month contract to design a revolutionary remote-controlled nano air vehicle (NAV) that will collect military intelligence indoors and outdoors on the urban battlefield.

Lockheed Martin Advanced Technology Laboratories (ATL) leads a team that will design a remote-controlled NAV, similar in size and shape to a maple tree seed. A chemical rocket enclosed in its one-bladed wing will power a sensor payload module more than 1,100 yards. Delivered from a hover and weighing up to 0.07 ounces, the module will be interchangeable based on mission requirements. Besides controlling lift and pitch, the wing will also house telemetry, communications, navigation, imaging sensors, and battery power. The NAV will be about 1.5 inches long and have a maximum takeoff weight of about 0.35 ounces.

In typical operation, a warfighter will launch the NAV and fly it toward the target by viewing its flight path through a camera embedded in the wing. Like a maple tree seed, the one-bladed device will rotate in flight, but its camera will provide a stable forward view and transmit images back to a small, hand-held display. As the system matures, a simple autopilot aboard the NAV will provide limited autonomous operations. Once the NAV delivers its payload, it will return to the warfighter for collection and refurbishment.

According to James Marsh, ATL director, designing and building such a small device will require revolutionary manufacturing technologies to integrate near-microscopic components into the airframe. But even the airframe will require a challenging combination of new and emerging technologies.

“The challenges are both exciting and daunting, because some of the technologies vital to our success have yet to be discovered,” Marsh said. “We know going in that we need some of the best minds in manufacturing technology and in the development and integration of highly sophisticated, software-driven, control technologies and mission systems.”

The contract will fund conceptual design and risk reduction using prototypes of the engine, airframe, flight control system, and communications system as well as computer models of the guidance system and sensors. Following a successful preliminary design review planned for summer 2007 and a sequence of go/no-go tests, DARPA may fund an additional 18-month period during which Lockheed Martin will design and test a flying prototype.

Lockheed Martin ATL leads a team that includes Lockheed Martin Advanced Development Programs (Skunk Works), Lockheed Martin Advanced Technology Center, the Lockheed

Martin-managed Sandia National Laboratories, AeroCraft, ATK Thiokol and the University of Pennsylvania.

Lockheed Martin's NAV program is part of a DARPA effort from its Defense Sciences Office to improve the quality, quantity, and reliability of information gathered and transmitted by unattended ground sensors. The effectiveness of these sensors may be dependent on their precise location. Achieving optimal monitoring and communication often requires precise deployment of sensors.

Headquartered in Bethesda, Md., Lockheed Martin employs about 135,000 people worldwide and is principally engaged in the research, design, development, manufacture, integration and sustainment of advanced technology systems, products and services.

# # #

Media Contact:
Stephen P. O'Neill, (856) 792-9815
e-mail: soneill@atl.lmco.com

For information on Lockheed Martin Corporation, visit:
www.lockheedmartin.com

APPENDIX H: MISCELLANEOUS SPSS OUTPUT DATA

```
T-TEST
  /TESTVAL = 0
  /MISSING = ANALYSIS
  /VARIABLES = Credibility Ease_of_Use Usefulness
  /CRITERIA = CI(.95) .
```

T-Test

```
[DataSet1] C:\Program Files\SPSS Evaluation\mscao-three-factors.sav
```

One-Sample Statistics

	N	Mean	Std. Deviation	Std. Error Mean
Credibility	357	3,44	,942	,050
Ease_of_Use	360	3,46	,850	,045
Usefulness	359	3,63	,887	,047

One-Sample Test

	Test Value = 0					
	T	df	Sig. (2-tailed)	Mean Difference	95% Confidence Interval of the Difference	
	Lower	Upper	Lower	Upper	Lower	Upper
Credibility	68,988	356	,000	3,440	3,34	3,54
Ease_of_Use	77,197	359	,000	3,458	3,37	3,55
Usefulness	77,617	358	,000	3,632	3,54	3,72

Paired Samples Correlations

		Paired Differences					T	df	Sig. (2-tailed)
		Mean	Std. Deviation	Std. Error Mean	95% Confidence Interval of the Difference			Std. Deviation	Std. Error Mean
					Lower	Upper			
Pair 1	Credibility - Ease_of_Use	-,014	1,051	,056	-,123	,095	-,252	356	,801
Pair 2	Credibility - Usefulness	-,185	,998	,053	-,289	-,081	-3,504	355	,001

```
T-TEST
  PAIRS = Credibility Credibility  WITH Ease_of_Use Usefulness (PAIRED)
  /CRITERIA = CI(.95)
  /MISSING = ANALYSIS.
```

T-Test

```
[DataSet1] C:\Program Files\SPSS Evaluation\mscao-three-factors.sav
```

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	Credibility	3,44	357	,942	,050
	Ease_of_Use	3,45	357	,852	,045
Pair 2	Credibility	3,44	356	,940	,050
	Usefulness	3,63	356	,890	,047

```
GET
  FILE='C:\Program Files\SPSS Evaluation\mscao-three-factors.sav'.
DATASET NAME DataSet1 WINDOW=FRONT.
FREQUENCIES
  VARIABLES=Credibility Ease_of_Use Usefulness
  /STATISTICS=STDDEV VARIANCE SEMEAN MEAN MEDIAN
  /HISTOGRAM  NORMAL
  /ORDER=  ANALYSIS .
```

Frequencies

```
[DataSet1] C:\Program Files\SPSS Evaluation\mscao-three-factors.sav
```

Statistics

		Credibility	Ease_of_Use	Usefulness
N	Valid	357	360	359
	Missing	3	0	1
Mean		3,44	3,46	3,63
Std. Error of Mean		,050	,045	,047
Median		4,00	4,00	4,00
Std. Deviation		,942	,850	,887
Variance		,888	,722	,786

Frequency Table

Credibility

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Strongly disagree	14	3,9	3,9	3,9
	Disagree	40	11,1	11,2	15,1
	Neither	110	30,6	30,8	45,9
	Agree	161	44,7	45,1	91,0
	Strongly agree	32	8,9	9,0	100,0
	Total	357	99,2	100,0	
Missing	System	3	,8		
Total		360	100,0		

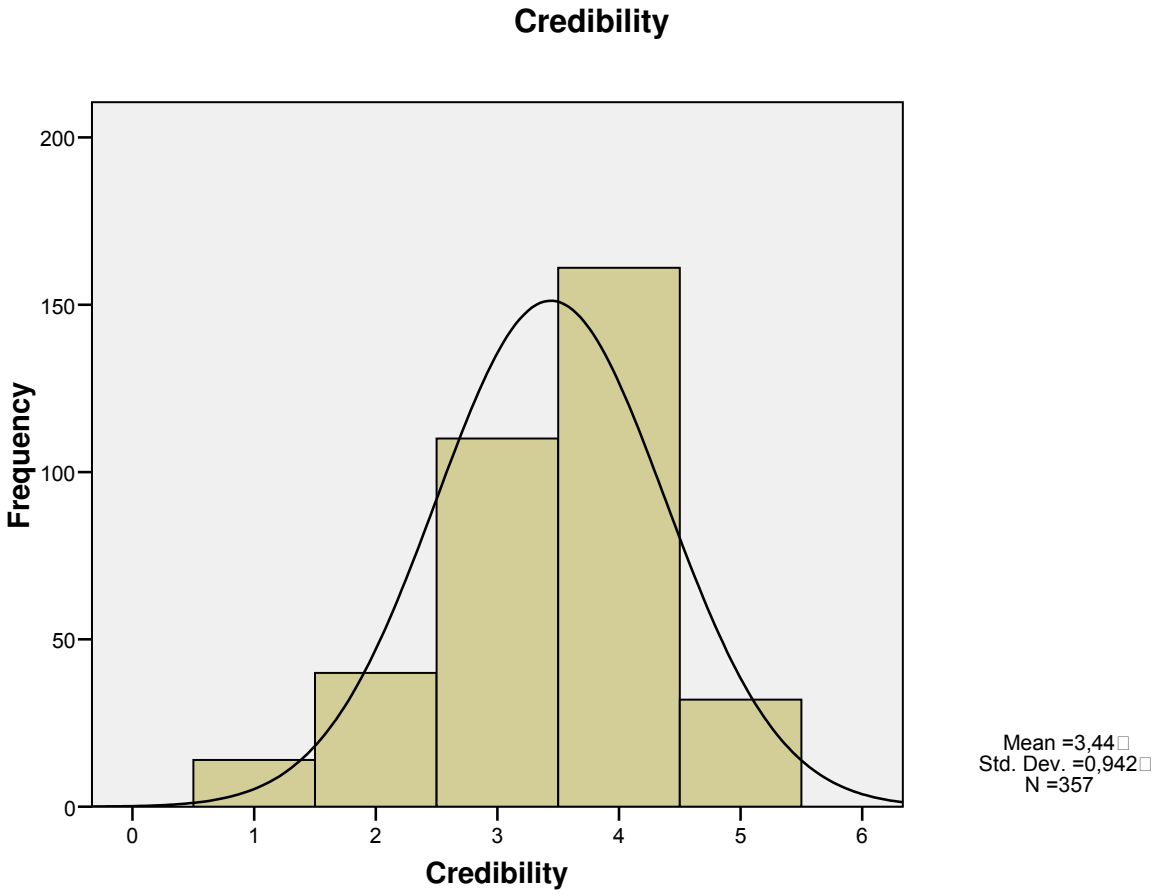
Ease_of_Use

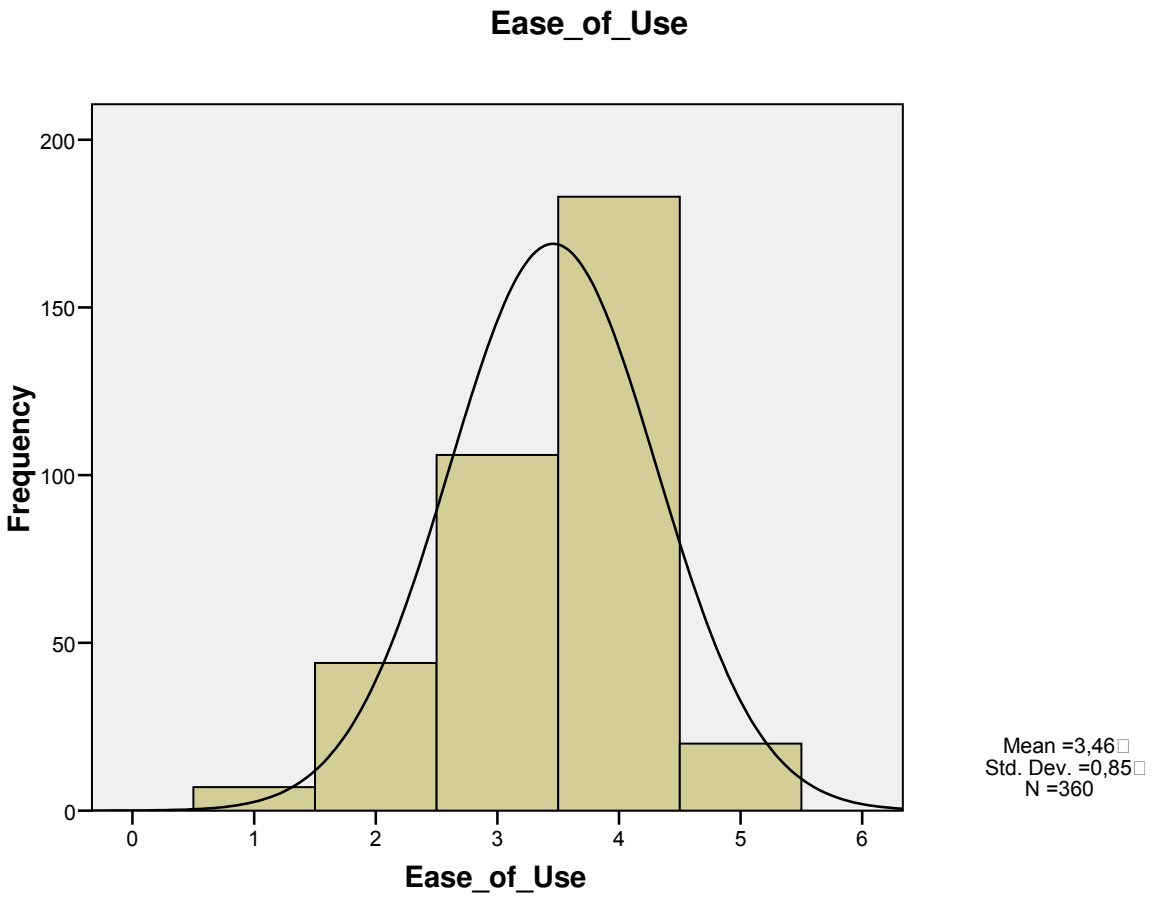
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	strongly disagree	7	1,9	1,9	1,9
	Disagree	44	12,2	12,2	14,2
	Neither	106	29,4	29,4	43,6
	Agree	183	50,8	50,8	94,4
	strongly agree	20	5,6	5,6	100,0
	Total	360	100,0	100,0	

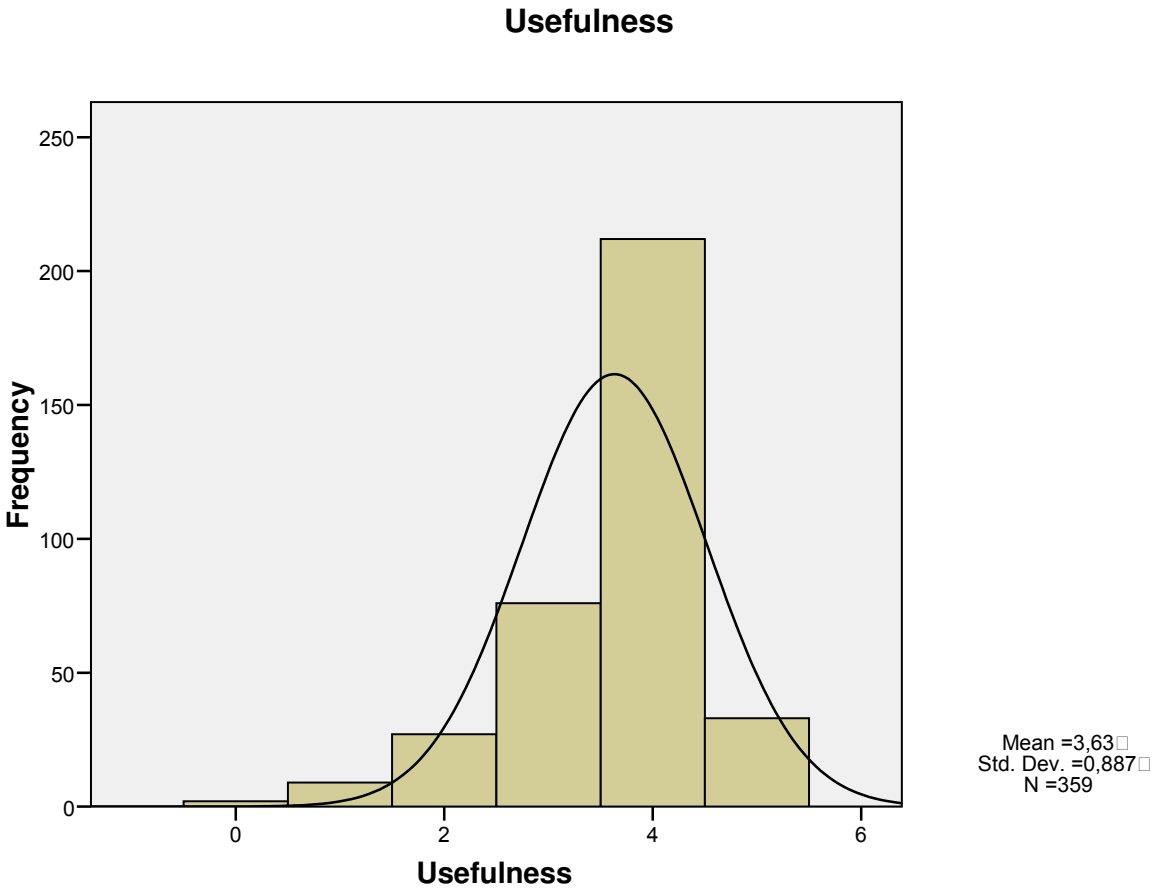
Usefulness

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Blank	2	,6	,6	,6
	Strongly disagree	9	2,5	2,5	3,1
	Disagree	27	7,5	7,5	10,6
	Neither	76	21,1	21,2	31,8
	Agree	212	58,9	59,1	90,8
	Strongly agree	33	9,2	9,2	100,0
	Total	359	99,7	100,0	
Missing	System	1	,3		
Total		360	100,0		

Histogram


Credibility
Frequency
200
150
100
50
0
0
1
2
3
4
5
6
Credibility
Mean =3,44
Std. Dev. =0,942
N =357


Ease_of_Use
Frequency
200
150
100
50
0
0
1
2
3
4
5
6
Ease_of_Use
Mean =3,46
Std. Dev. =0,85
N =360


Usefulness
250
200
150
100
50
0
Frequency
0
2
4
6
Usefulness
Mean =3,63
Std. Dev. =0,887
N =359

```
SUMMARIZE
  /TABLES=gender rank major
  /FORMAT=VALIDLIST NOCASENUM TOTAL LIMIT=100
  /TITLE='Case Summaries'
  /MISSING=VARIABLE
  /CELLS=COUNT NPCT.
```

Summarize

[DataSet2] D:\Model for Safer Cyber-Assisted Olfaction.sav

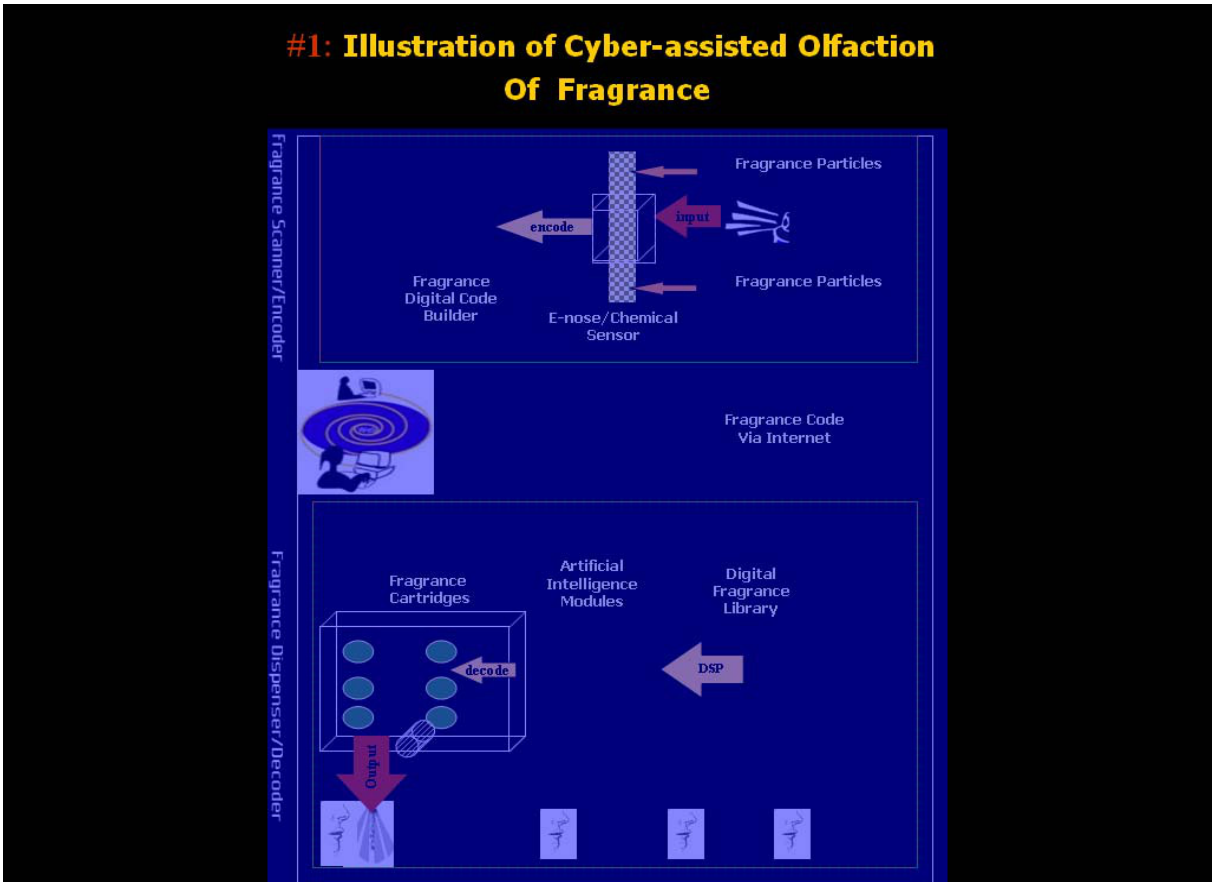
Case Summaries (a)

	Gender	Academic Level	Major
1	Male	Undergraduate	Electronics
2	Male	Undergraduate	.
3	Female	Undergraduate	Electronics
4	Male	Undergraduate	Electronics
5	Male	Undergraduate	Electrical and Computer
6	Male	Undergraduate	Electrical and Computer
7	Male	Undergraduate	Electrical and Computer
8	Female	Undergraduate	Electrical and Computer
9	Male	.	Electrical and Computer
10	Male	Undergraduate	Electronics
11	Male	Undergraduate	Electrical and Computer
12	Male	.	Electrical and Computer
13	Female	Undergraduate	Electrical and Computer
14	Male	Undergraduate	Electrical and Computer
15	Male	Undergraduate	Electrical and Computer
16	Male	.	Electrical and Computer
17	Male	Undergraduate	Electronics
18	Male	Undergraduate	Electronics
19	Female	.	Civil
20	Male	Undergraduate	Civil
21	Male	Undergraduate	Electrical and Computer
22	Male	Undergraduate	Electronics
23	Male	.	Electronics
24	Female	Undergraduate	Electrical and Computer
25	Male	Undergraduate	Electronics
26	Male	Undergraduate	Electronics
27	Male	Undergraduate	Electrical and Computer
28	Female	Undergraduate	Electrical and Computer
29	Male	Graduate	Electrical and Computer
30	Male	Undergraduate	Electrical and Computer
31	Male	Undergraduate	Electrical and Computer
32	Male	Graduate	Electrical and Computer
33	Male	Undergraduate	Electronics
34	Male	.	Electronics
35	Male	Graduate	Electronics
36	Male	Graduate	Mechanical
37	Male	Undergraduate	Electrical and Computer
38	Female	Undergraduate	Electrical and Computer
39	Male	Graduate	Electrical and Computer
40	Male	Graduate	Electrical and Computer
41	Male	Graduate	Electrical and Computer
42	Male	Undergraduate	Electrical and Computer
43	Female	Undergraduate	Electronics
44	Male	Graduate	Electrical and Computer
45	Female	Undergraduate	Electrical and Computer
46	Male	Undergraduate	Electrical and Computer
47	Male	.	Electrical and Computer
48	Male	Undergraduate	Electrical and Computer
49	Female	Undergraduate	Electrical and Computer
50	Female	Undergraduate	Electronics
51	Male	Undergraduate	Electronics
52	Male	Undergraduate	Electronics
53	Male	Undergraduate	Electronics
54	Male	Undergraduate	Electronics
55	Female	Graduate	Electronics
56	Male	Undergraduate	Electronics
Tot	**44+12=56**	**40+9 =49**	**21+ 30+2+1+1= 55**

a Limited to first 100 cases.

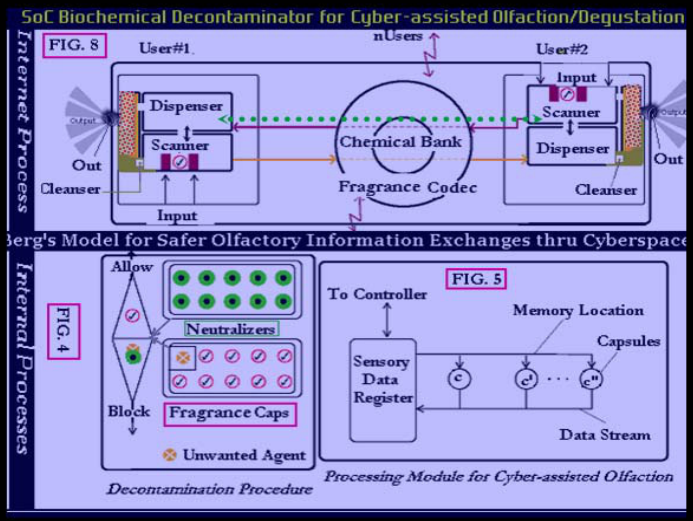
APPENDIX I: POWERPOINT SLIDES OF MULTIMEDIA COMPONENTS

SCENARIO-1

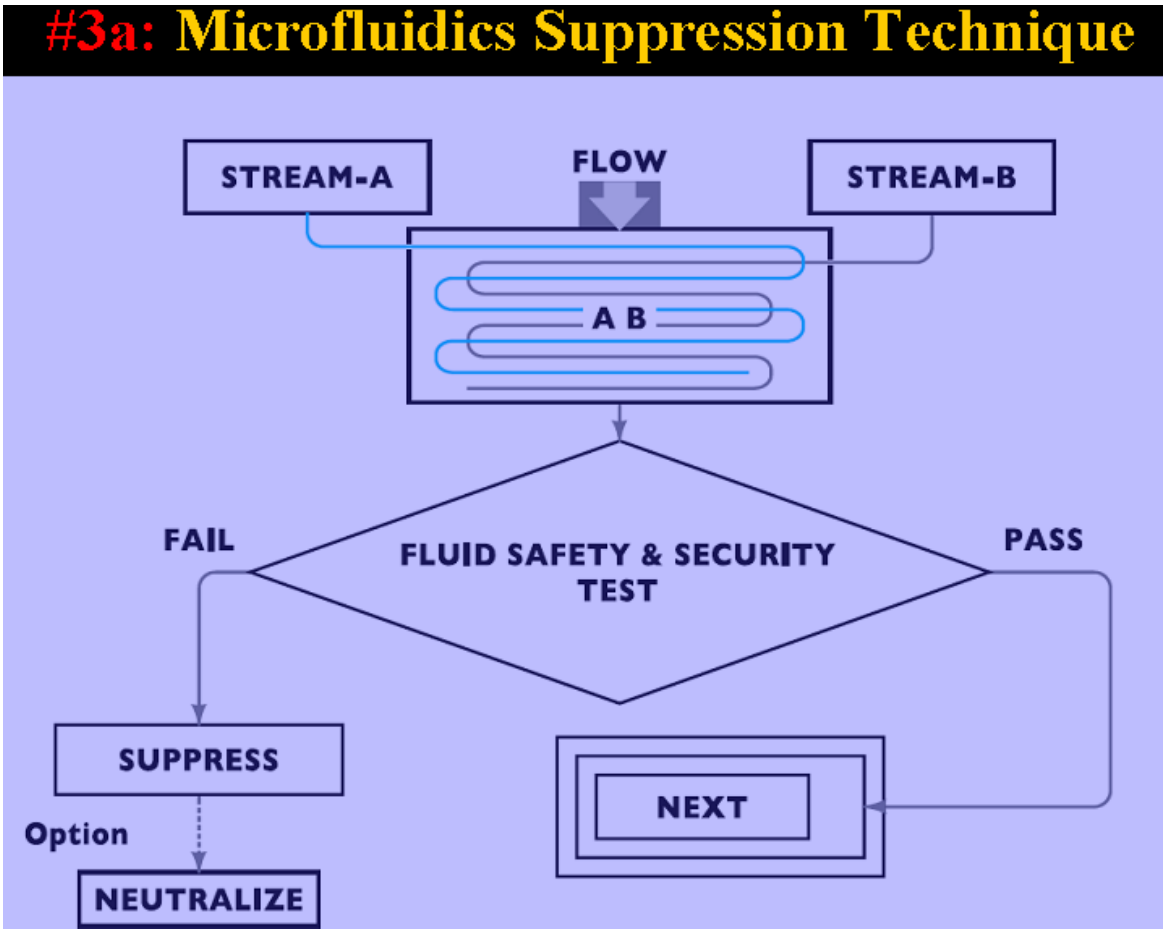


SCENARIO-2

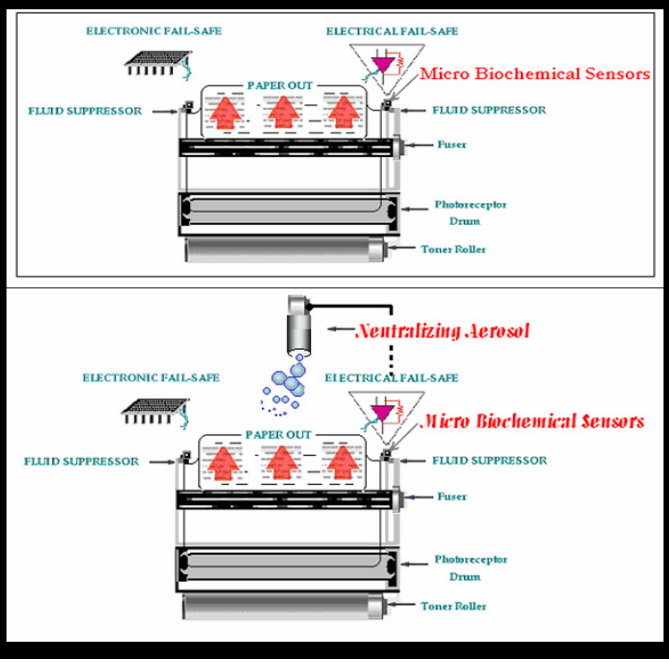
#2: Internet Applications



SCENARIO-3

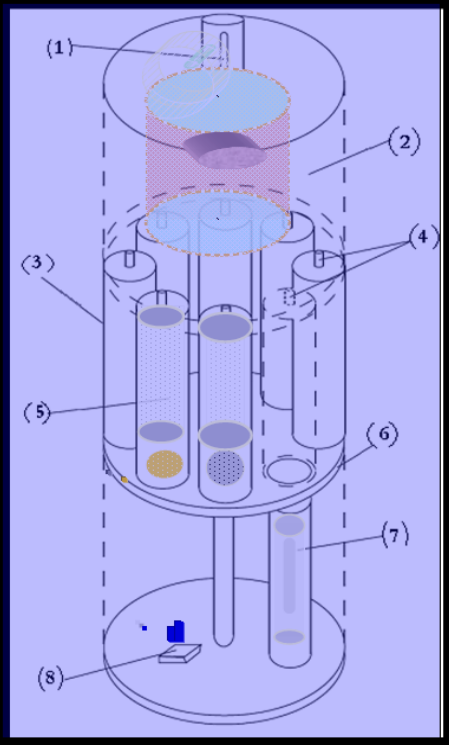

#3a: Microfluidics Suppression Technique
STREAM-A
FLOW
STREAM-B
A B
FAIL
FLUID SAFETY & SECURITY TEST
PASS
SUPPRESS
Option
NEUTRALIZE
NEXT

#3b: MSCAO in Printing Devices

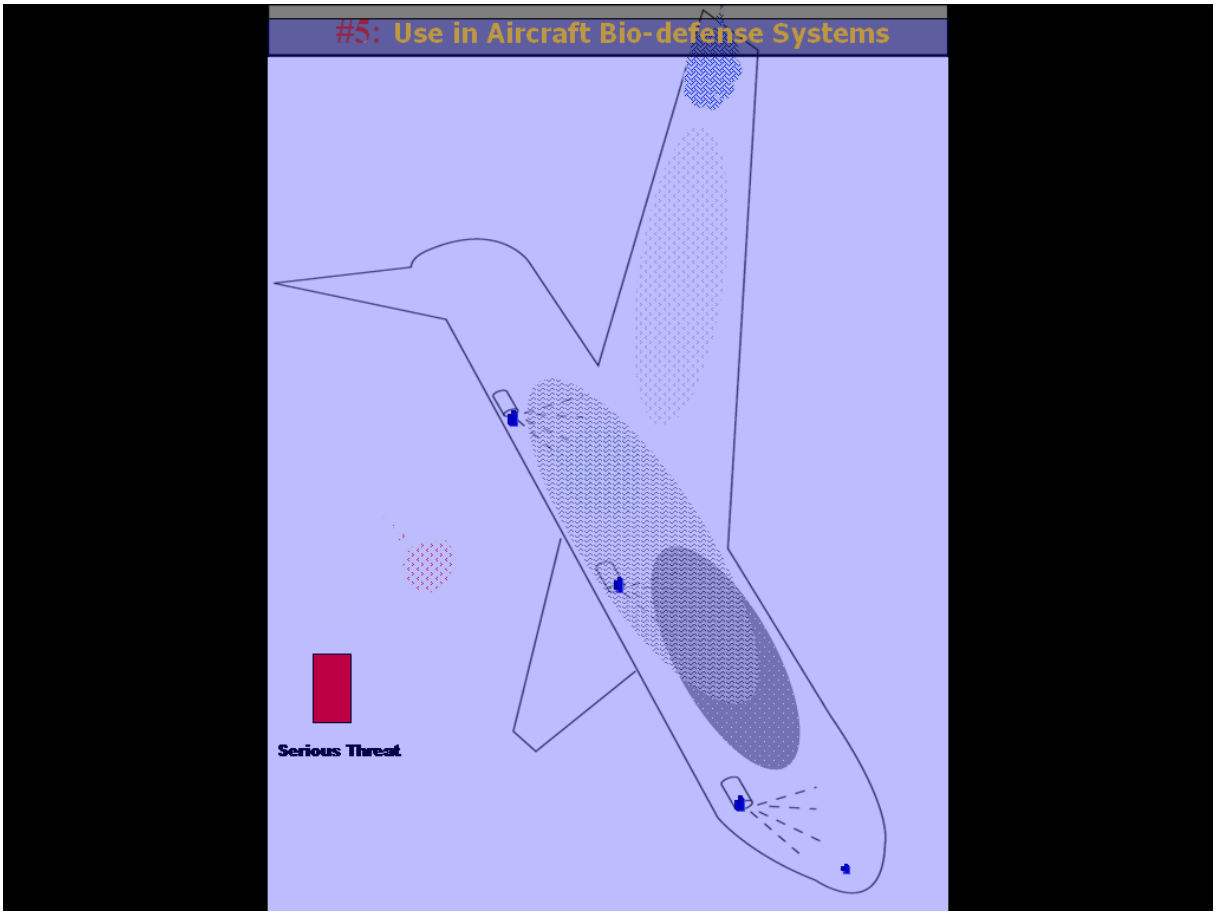


SCENARIO-4

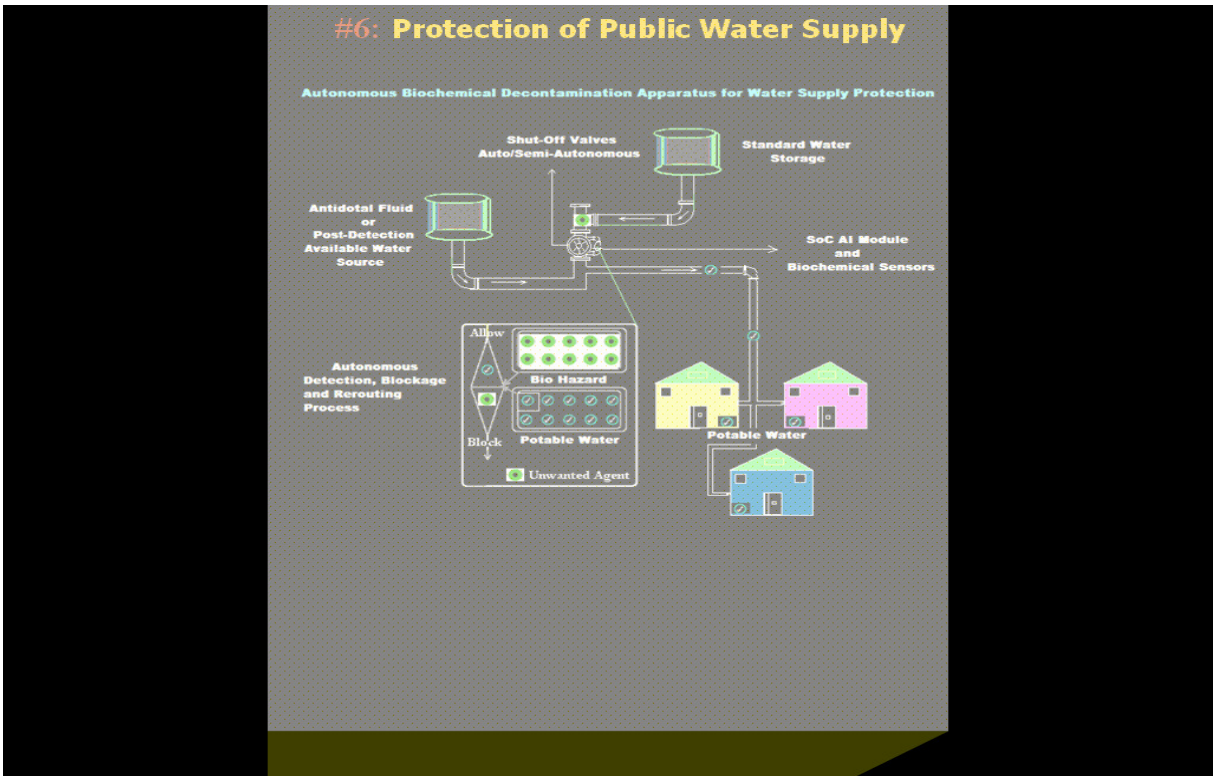
#4: Hyacinthe's Model of Autonomous Bio-Chemical Decontamination



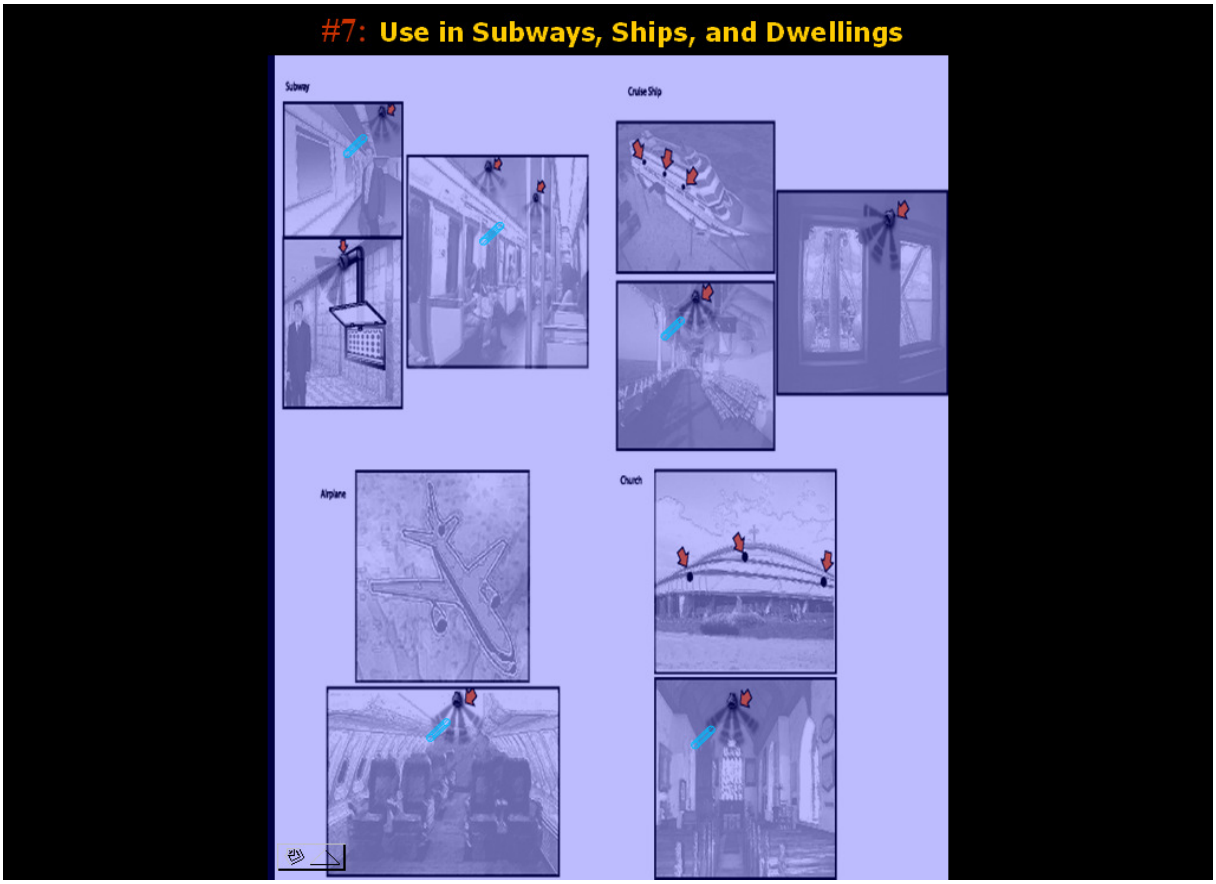
SCENARIO-5



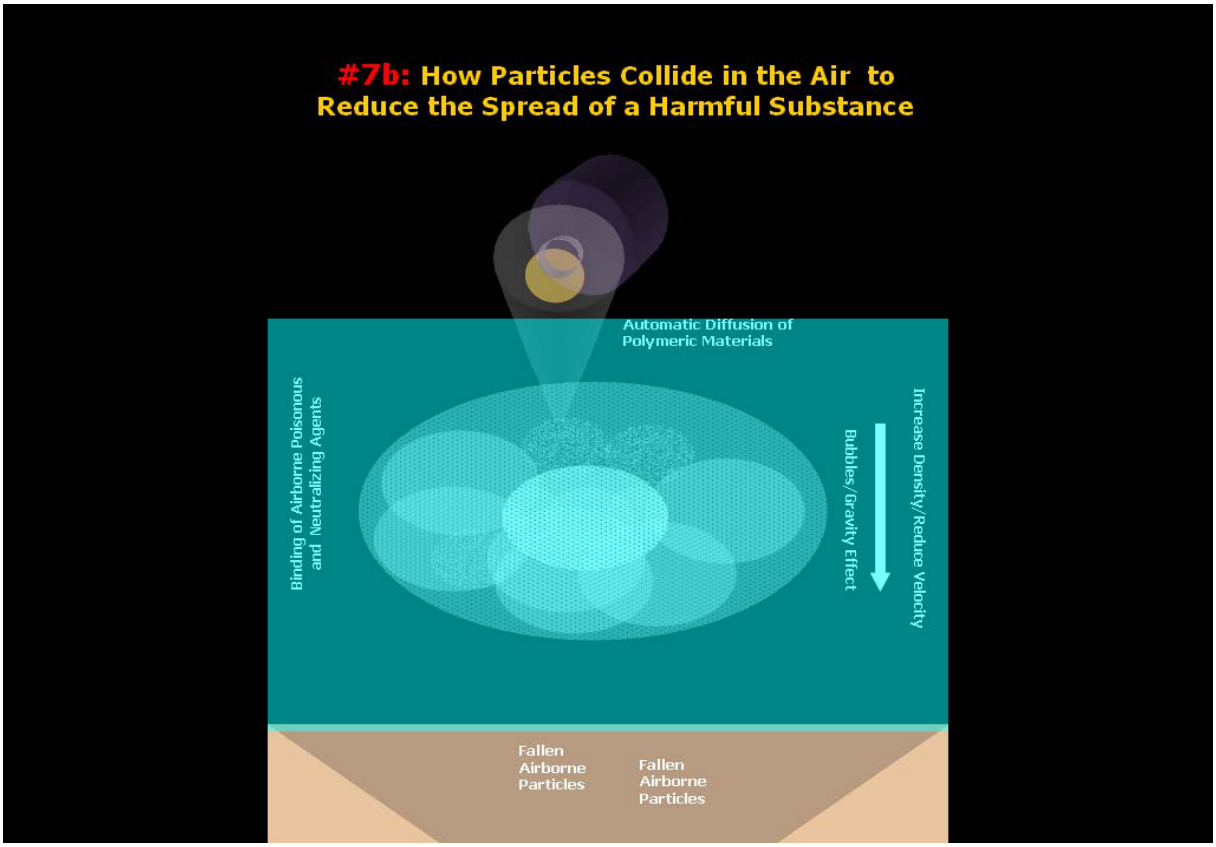
SCENARIO-6


#6: Protection of Public Water Supply
Autonomous Biochemical Decontamination Apparatus for Water Supply Protection
Shut-Off Valves
Auto/Semi-Autonomous
Standard Water
Storage
Antidotal Fluid
or
Post-Detection
Available Water
Source
SoC AI Module
and
Biochemical Sensors
Autonomous
Detection, Blockage
and Rerouting
Process
Allow
Bio Hazard
Block
Potable Water
Unwanted Agent
Potable Water

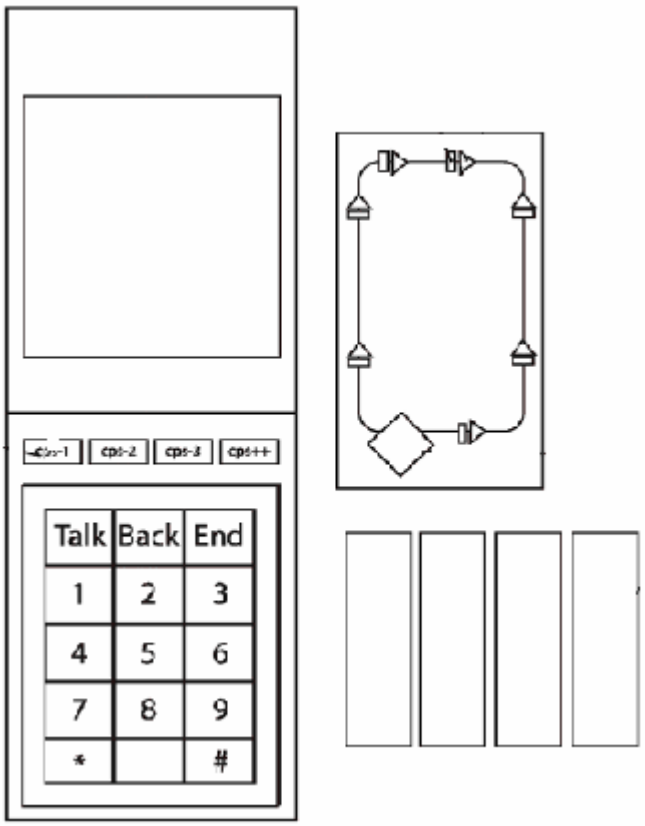
SCENARIO-7


#7: Use in Subways, Ships, and Dwellings
Subway
Cruise Ship
Airplane
Church

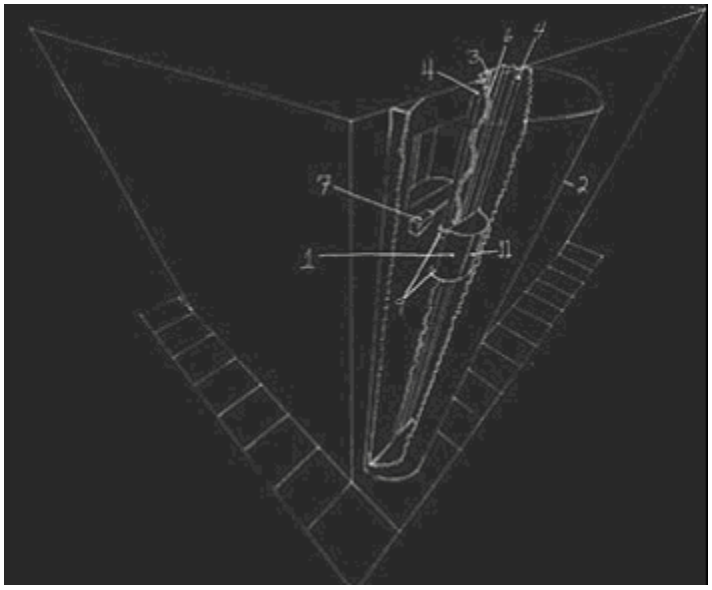
SCENARIO-7b

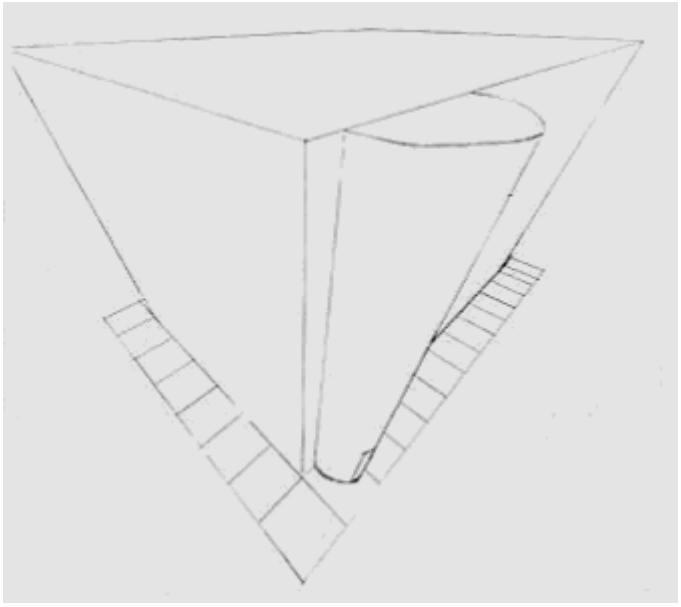

#7b: How Particles Collide in the Air to Reduce the Spread of a Harmful Substance
Automatic Diffusion of Polymeric Materials
Binding of Airborne Poisonous and Neutralizing Agents
Bubbles/Gravity Effect
Increase Density/Reduce Velocity
Fallen Airborne Particles
Fallen Airborne Particles

APPENDIX J: RESEARCHER'S VARIOUS PROPOSED INNOVATIONS

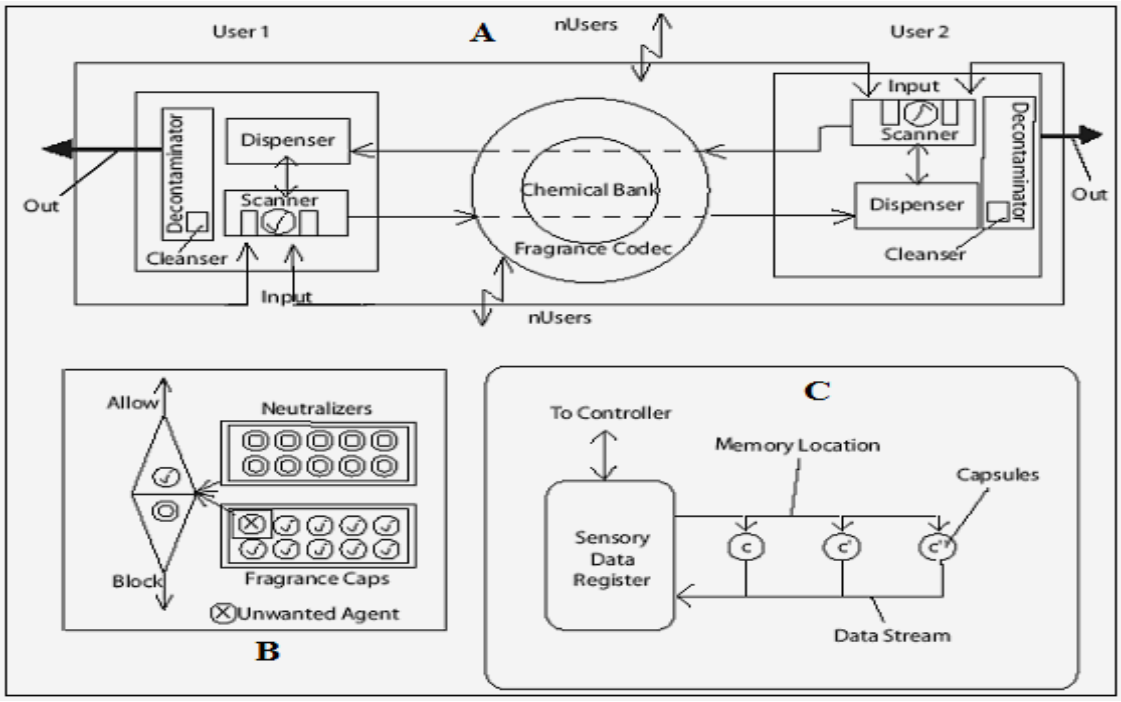


The Universal Cellular Board is proposed with a digital security diagnostic bus allowing the scanning of the physical layers of the integrated circuits for digital security breaches such as espionage and sophisticated terror attacks. For further information, see US-60/601658035.

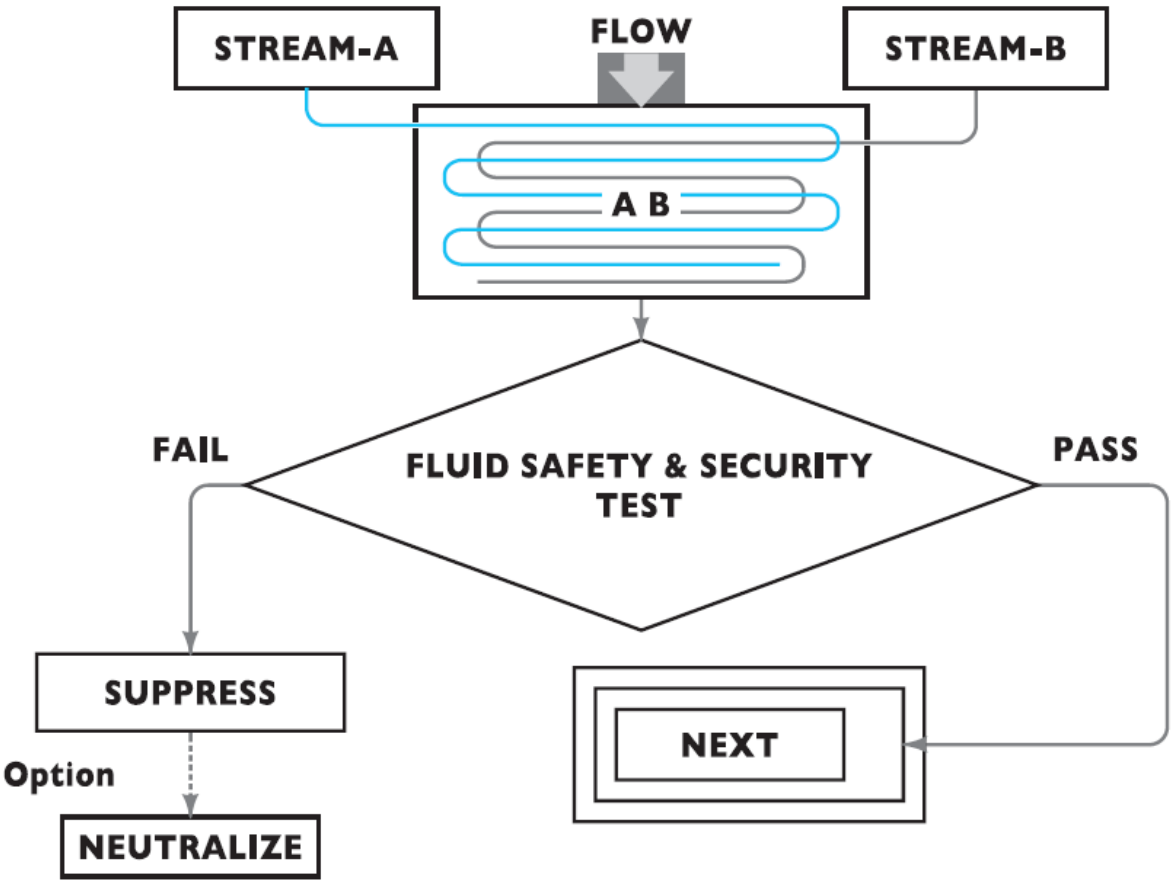




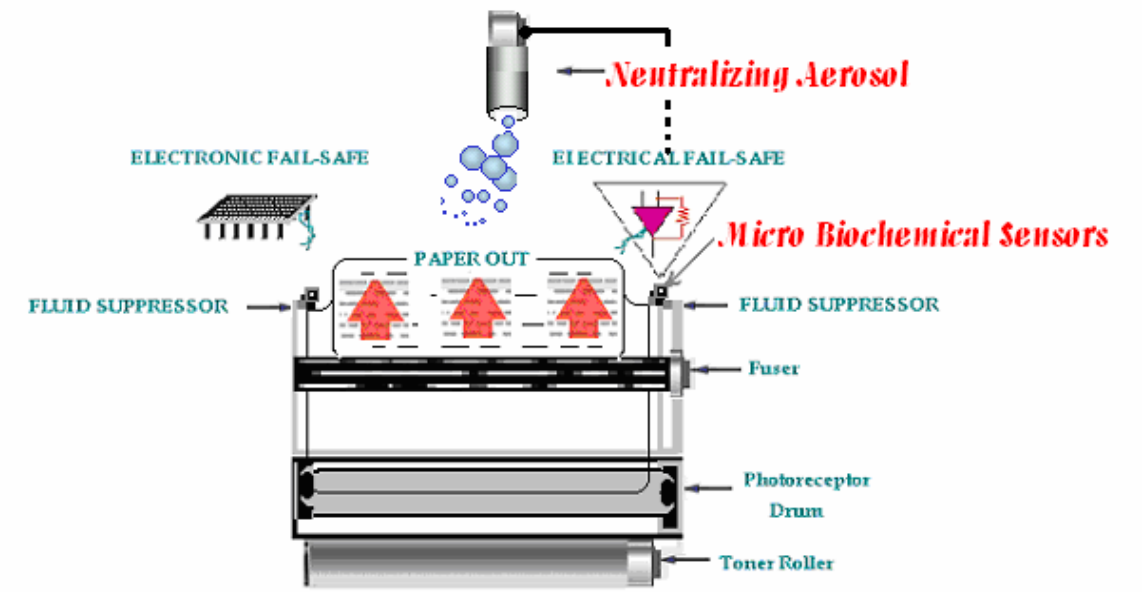
Emergency Rescue Vehicle (Hyacinthe, 2005b, US-60/634,637): Rapid mass evacuation system from high altitudes (connected to underground routes and/or mobile rescue vehicles via a tube or an accordion-like protective envelop) in the event of biochemical attack or major fire (see the associated patent publication for explanation of numerical markers).



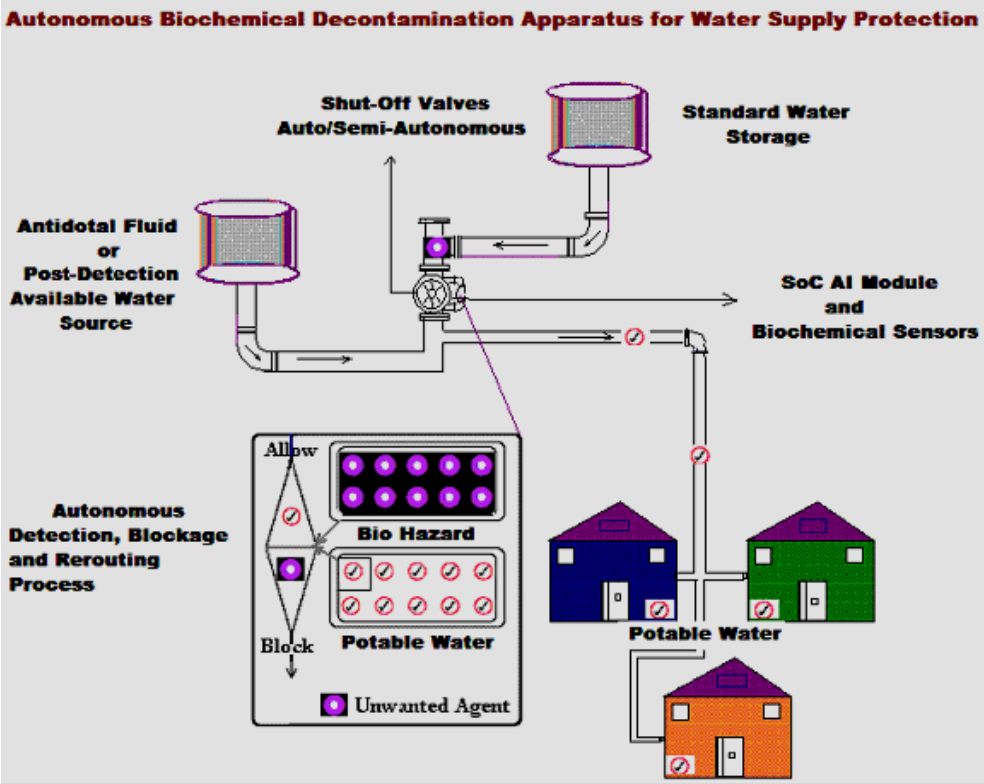
Model for safer cyber-assisted olfaction (Hyacinthe, 2006b): (A) Cyber-assisted olfactory information exchange between two users; (B) Suppression and neutralization in micro systems; (C) Sensory data protocols (US-60/700,708).



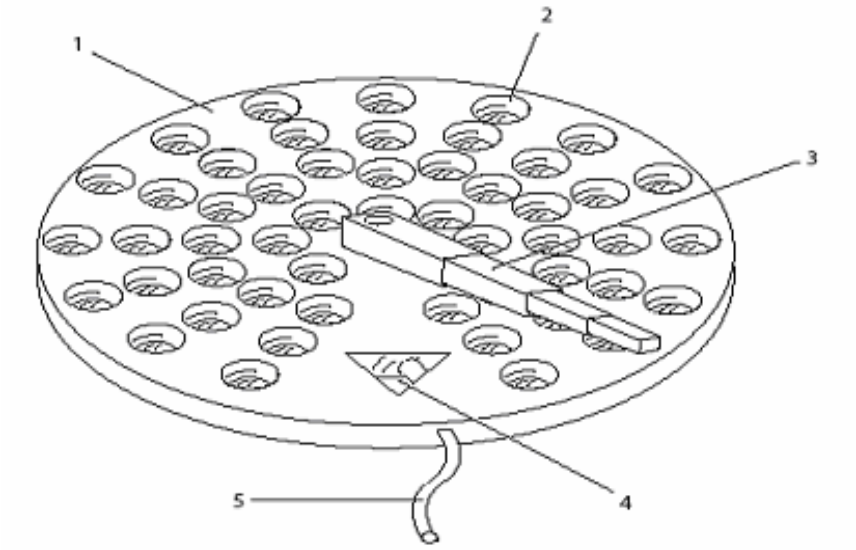
The process of microfluidics suppression is illustrated with two fluid streams A and B. In this example, A and B are mixed in a chamber. The security diagnostic test is initiated by a biosensor. If the compound AB fails the test, then a signal is sent to suppress fluid circulation; else, no action is taken. It is important to note that the same principle applies to a plurality of fluid streams (A to Z). The optional diffuser may disperse an antibody as a mitigating agent (Hyacinthe, 2006; provisional patent application #US-60/814320).



In this example, a biochemical warfare agent is detected; and an antibody has been diffused to mitigate its harmful effects. The system is embeddable in printers, fax machines, photocopiers, and related devices. A similar process will work to secure computers or cell phones with aromatic features. This image is extracted from provisional patent application number US-60/814320 (Hyacinthe, 2006). Printer proposed as the prototype of a more complex system.



This example illustrates a countermeasure for the public water supply (that suspends the water flow and warns subscribers), in the event of sophisticated bio-terror attack.



Spherical Storage Unit for Microsystems: (1) Perforated disk; (2) Chemical containers; (3) Retractable robotic arm; (4) Mixing chamber; and (5) Aerosol exhaust (US-60/700,708).

APPENDIX K: WARNINGS AND MAJOR ATTACKS

It is fair to say that U.S. authorities have been fortunate enough to receive warnings about the most sophisticated attacks launched against them. Yet, a bipartisan investigation of 9/11 terrorist attacks blamed the failure of the U.S. intelligence community on a "lack of imagination" (The 9/11 Commission Report, 2004).

- Post-attack information about Pearl Harbor (the Japanese's successful attack against the United States Navy in Hawaii) was blurry, yet existent.
- Although conflicting, warnings related to the attack on the USS Liberty (Latham, 2003, p. 289), existed.
- Authorities were privy to tremendous pre-attack information regarding the *911 attack* on America (commercial airlines were used as missiles to destroy the New York Twin Towers, hit the Pentagon, and to destroy other critical infrastructures).
- Pre-war intelligence regarding the Iraqi conflict (which threatens to destabilize an already "shaky" Middle East region) pointed to very high risks. Unfortunately, the number and type of casualties resulting from the Iraq War continued to grow during the redaction of this report. The 'outing' of a CIA official (Valerie Plame) and the criminal conviction of a powerful attorney, Scooter Libby, exemplified how far many U.S. officials went and how wrong others have been in their pursuit. Libby is former chief of staff of Vice President Dick Chenney, one of his most trusted advisers.
- Continuous warnings related to the Vietnam War had been documented.

REFERENCES

Aas, P. (2003). Future considerations for the medical management of nerve agent intoxication. *Prehosp. Disast. Med., 18*(3), 208-216.

Adams, J. (1998). *The next world war: Computers are the weapons and the front line is everywhere*. Simon & Schuster, New York: Simon & Schuter.

Ahlqvist, T. (2005). From information society to biosociety? On societal waves, developing key technologies, and new professions. *Technological Forecasting and Social Change*, *72*, 501-519.

Al-Gahtani, S. (2001). The applicability of TAM outside North America: An empirical test in the United Kingdom. *Information Resources Management Journal*, *14*(3), 37-46.

Anastasi, A. (1986). Evolving concepts to test validation. *Annual Review of Psychology*, *37*, 1-15.

Anderson, D. (2001). *Army's Commitment to Supporting the Homeland Security Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive Weapon Terrorist Threat: Can the Reserve Components Meet the Requirement by Themselves?* Carlisle Barracks, PA: Army War College.

Armstrong, S. (1978). *Long-Range Forecasting: From Crystal Ball to Computer*. New York: John Wiley.

Babbie, E. (2001). *The practice of social research*. Australia: Wadsworth.

Baeumner, A., Humiston, M., Montagna, R., and Durst, A. (2001). Detection of Viable Oocysts of Cryptosporidium parvum Following Nucleic Acid Sequence Based Amplification. *Anal. Chem.*, *73,* 1176-1180.

Bandura, A. (1986). *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, N.J: Prentice-Hall.

Barfield, W., and Danas, E. (1995). Comments on the Use of Olfactory Displays for Virtual Environments. *Presence*, *5*(1), 109-121.

Bass, F. (1969). A New Product Growth Model for Consumer Durables. *Management Science*, *13*(5), 215-227.

Basu, A., and Fabre, M. (1992). Fractals and Critical Information Susceptibility in a Simulation of Spatial Diffusion of Innovations. *Journal of Scientific and Industrial Research, 51*(xx), xx, 251-256.

Becker, H. (1971). *Sociological work*. London: Allen Lane.

Benbasat, I., and Dexter, A. (1986). An Investigation of the Effectiveness of Color and Graphical Presentation Under Varying Time Constraints. *MIS Quarterly, 10*, (1), 59-84.

Bero, LA., Grilli R., Grimshaw JM., *et al*. (1998). Closing the gap between research and practice: an overview of systematic reviews of interventions to promote the implementation of research findings. *BMJ*, *317*, 465-468.

Bertel, S., Freksa, C., and Vrachliotis, G. (2004). Aspectualize and conquer in architectural design. In J. S. Gero, B. Tversky, and T. Knight (Eds), *Visual and Spatial Reasoning in Design III* (pp. 255–279). University of Sydney, Australia: Key Centre of Design Computing and Cognition.

Bertel, S., Vrachliotis, G., and Freksa, C. (2007). Aspect-oriented building design: Toward computer-aided approaches to solving spatial constraints in architecture. In L. G. Allen, (Eds.), *Applied Spatial Cognition: From Research to Cognitive Technology* (pp. 75-102). Mahwah, NJ: Lawrence Erlbaum Associates.

Bewley, W., Roberts, T., Schoit, D., and Verplank, W. (1983). Human Factors Testing in the Design of Xerox's 8010 'Star' Office Workstation. *Proceedings of the CHI 1983 Conference on Human Factors in Computing Systems*, 72-77.

Bishop, M., and Goldman, E. (2003).The Strategy and Tactics of Information Warfare. *Contemporary Security Policy 24*, 113-139.

Boahene, K. (1995). *Innovation Adoption as a Socio-Economic Process: The Case of the Ghanian Cocoa Industry*. Amsterdam: Thesis Publishers.

Bomsdorf, B. (1996). Task as Agents: prototyping task models. *Proceedings of Sixth Australian Conference on Computer-Human Interaction*, 286-293.

Bondonio, D. (1998). Predictors of Accuracy in Perceiving Informal Social Networks. *Social Networks*, *20*(4), 301-330.

Bowen, W. (1986). The Puny Payoff from Office Computers. *Fortune, 5*, 20-24.

Braman, S. (1989). Defining Information. *Telecommunications Policy, 13*, 233-242.

Brown, K., Taylor, K., Jing, Y., and Khan, T. (2002). Intelligent Agents an Approach to Supporting Multiple Model Based Training Systems*. Fith International Proceedings on Intelligent Tutoring Systems*. San Sebastian. Spain. Available: www.http://monet.aber.ac.uk:8080/monet/docs/pdf_files/its_02/b_t_j_k.pdf

Brown, S. (1998). *A decision theoretic approach for interface agent development*. (PhD Thesis). Air Force Institute of Technology. USA: Air University.

Brown, S. A., Massey, A. P., Montoya-Weiss, M. M., and Burkman, J. R. (2002). Do I really have to? User acceptance of mandated technology. *European Journal of Information Systems, 11*(4), 283-295.

Brunswick, E. (1956). *Perception and the Representative Design of Psychological Experiments*. Berkeley: Univ. Calif. Press.

Bryman, A. (1984). The debate about quantitative and qualitative research: A question of method or epistemology? *The British Journal of Sociology, 35* (1), 75-92.

Buck, L.B. (1996). Information coding in the mammalian olfactory system. *Symp. Quant. Biol., 61*,147-155.

Buckland, M. (1991). Information as Thing. *JASIS, 42* (5), 351-360.

Bush, V. (1945). As We may Think. *Atlantic Monthly, 176*(i), 101-108.

Cain, W., and Murphy, C. (1980). Interaction between chemoreceptive modalities of odor and irritation. *Nature, 3,* 255-257.

Capurro, R. Hjørland, B. (2003).The concept of information. *Annual Review of Information Science and Technology (ARIST), 37*, 343-411.

Carley, K. (1996). Communicating New Ideas: The Potential Impact of Information and Telecommunication Technology. *Technology in Society, 18*(2), 219-230.

Carroll, JM. (1992). Creating a design science of human-computer interaction. In A Bensoussan, J-P Verjus (Eds.), *Future Tendencies in Computer Science, Control, and Applied Mathematics: 25th Anniversary of INRIA* (pp. 205-215). New York: Springer-Verlag.

Charmaz, K. (2000). Grounded Theory: Objectivist and Constructivist Methods. In N. Denzin and Y. Lincoln (Eds.), *Handbook of Qualitative Research* (pp. 509–536). Thousand Oaks, CA: Sage.

Chatterjee, A. N., and Aluru, N. R. (2005). Combined circuit/device modelling simulation of integrated microfluidic systems. *J. Microelectromechanical Syst., 14*, 81-95.

Chatterjee, A.N., Aluru, N.R., and Beebe, D.J. (2005). Development and modeling of electrically triggered hydrogels for microfluidic applications. *Journal of Microelectromechanical Systems, 14*(5), 1198-1207.

Chau, P., and Hu, P. J. (2002). Investigating healthcare professionals' decisions to accept telemedicine technology: An empirical test of competing theories. *Information and Management, 39*(4), 297-311.

Chermack, T. J., and Lynham, S. A. (2002). Definitions and outcome variables of scenario planning. *Human Resource Development Review, 1*(3), 366-383.

Chermack, T., Lynham, S., and Ruona, W. (2001). A review of scenario planning literature. *Futures Res., 17*(2), 7-31.

Clark, R. (2003). *Intelligence Analysis*: *A Target-Centric Approach*. Washington D.C.: CQ Press.

Coffman, T., Greenblatt, S., and Marcus, S. (2004). Graph-based Technologies for Intelligence Analysis. *CACM, 47*(3), 45-47.

Cohen, J. (1988). *Statistical power analysis for the behavioral sciences*. Hillsdale: Lawrence Erlbaum Associates.

Collings, A., and Caruso, F. (1997). Biosensors: recent advances. *Rep. Prog. Phys., 60*, 1397-1445.

Cook, T.D., and Campbell, D.T. (1979). *Quasi-Experimentation: Design and analysis issues for field settings*. Boston: Houghton Mifflin Company.

Coyne, R., Park, H., and Wiszniewski, D. (2002). Design devices: digital drawing and the pursuit of difference. *Design Studies, 23*, 263-286.

Cresswell, J.W. (2002). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. London: Merrill Prentice-Hall.

Dariva, C., Coelho, L.A.F., and Oliveira, J.V. (1999). A Kinetic Approach for Predicting Diffusivities in Dense Fluid Mixtures, Fluid Phase. *Equilibria, 158*, 1045-1054.

DARPA (2007). *Nano Air Vehicles (NAVs)*. Available: http://www.darpa.mil/dso/thrust/matdev/nav.htm

Davies, H., and Nutley, S., and Walter, I. (2005). *Assessing the impact of social science research: conceptual, methodological and practical issues*. Available: http://www.odi.org.uk/RAPID/Events/ESRC/docs/background_paper.pdf

Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35*, 982-1003.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Davis, F.D., and Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. *International Journal of Human Computer Studies, 45*, 19-45.

Declassified Military Reports. (2005). *Chemical, Biological, and Nuclear Terrorism / Warfare: A Bibliography Chemical: Technical Reports (from the U.S. Naval Post Graduate School).* Available: http://library.nps.navy.mil/home/bibs/chemtech.htm

de Gelder, B., and Bertelson, P. (2003). Multisensory integration, levels of processing and ecological validity. *Trends in Cognitive Science 7*(10), 460– 467.

Dekker, M., and Olson, C. (1976). On choosing a test statistic in multivariate analysis of variance. *Psychological Bulletin, 83*, 579-586.

Denis, J., Hebert., Y, Langley, A., *et al*. (2002). Explaining diffusion patterns for complex health care innovations. *Health Care Manage Rev., 27*, 60-73.

Dey, I. (1993). *Qualitative data analysis: a user friendly guide for social scientists*. London: Routledge.

Dishaw, M.T., and Strong, D.M. (1999). Extending the technology acceptance model with the task-technology fit constructs. *Information and Management, 36* (1), 9-21.

DNI. (2007). *DNI Organization*. Available: http://dni.gov/aboutODNI/organization.htm

Dutton, W. (1997). *Information and Communication Technologies: Vision & Realities*. New York: Oxford University Press.

Edwards, P. (1996).*The closed world: Computers and the politics of discourse in cold war America*. The MIT Press, Cambridge, Massachusetts.

Eigen, M., and Rigler, R. (1994). Sorting single molecules: Application to diagnostics and evolutionary biotechnology. *Proceedings of the Natl. Acad. Sci., 91*, 6, 5740-5747.

Einstein, A. (1926). *Investigations on the theory of the Brownian movement*. Ed. R. Fürth, Tr. A. D.Cowper, London, Methuen.

Ewing, R., Atkinson, D., Eiceman. G., Ewing, G. (2001). A critical review of ion mobility spectrometry for the detection of explosives and explosive related compounds. *Talanta, 54*, 515–529.

Fair, R., Khlystov, A., Srinivasan, V., Pamula, V., and Weaver, K. (2004). Integrated chemical/biochemical sample collection, pre-concentration, and analysis on a digital microfluidic lab-on-a-chip platform. *Proceedings of SPIE Optics East*, 5591.

Fei, S., Chakrabarty, K., and Fair, R. (2006). Microfluidics-Based Biochips: Technology Issues, Implementation Platforms, and Design-Automation Challenges. *IEEE transactions on computer-aided design of integrated circuits and systems, 25* (2), 211-223.

Farrell, R., and Breimer, E. (2000). A task-based architecture for application-aware adjuncts. *Proceedings of International Conference of Intelligent User Interfaces' 2000*, 82 - 85.

Finke, R. A. (1990). *Creative imagery: Discoveries and inventions in visualization*. Hillsdale, NJ: Lawrence Erlbaum.

Fishbein, M., and Ajzen, I. (1975). *Belief, Attitude, Intention and Behavior: An Introduction to Theory and Research*. Reading, MA: Addison-Wesley.

Fogg, B.J. (2003). *Persuasive Technology: Using Computers to Change What We Think and Do. Sanfrancisco, CA: Morgan Kaufmann Publishers.*

Fowler, F. J. (1995). *Improving Survey Questions: Design and Evaluation*. Thousand Oaks, CA: Sage Publications.

Frankfort-Nachmias, C., and Nachmias, D. (1996). *Research Methods in the Social Sciences*, 5th ed. London: Edward Arnold.

Friedman, T. (2005). *The world is flat: The globalized world in the twenty-first century*. Strand, London: Penguin Group.

Frye-Mason, G., Kottenstette, R., Lewis, P., Heller, E., Manginell, R., Adkins, D., Dulleck, G., Martinez, D., Sasaki, D., Mowry, C., Matzke, C., and Anderson, L. (2000). Hand-Held Miniature Chemical Analysis System (μChemLab) for Detection of Trace Concentrations of Gas Phase Analytes, *Micro Total Analysis Systems*, *229*, 3.

Garst, R. and Gross, M. (2005). On Becoming an Intelligence Analyst. In D. Clift, *Learning with Professionals: Selected Works from the JMIC* (pp. 39-45). Washington DC: JMIC.

Gathegi, J. (2005). Officially-mandated disappearing information: The legal depublication phenomenon. *Government Information Quarterly*, *22*, 423-439.

Gefen, D., and Straub, D.W. (1997). Gender Differences in the perception and use of e-mail: An extension to the technology acceptance model. *MIS Quarterly*, *21* (4), 389-400.

Gefen, D., Karahanna, E., and Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly*, *27*(1), 51-90.

Ginzberg, M. (1981). Early Diagnosis of MIS Implementation Failure: Promising Results and Unanswered Questions. *Management Science*, *27*, 4, 459-478.

Glasser, B., and Strauss, A. (1967). *The discovery of grounded theory.* Chicago: Aldine.

Gould, J. D., and Lewis, C. (1985). Designing for Usability: Key Principles and What Designers Think. *Communications of the ACM*, *28*(3), 300-311.

Grabow, C. L. (1991). *Implications and Effects of Advanced Biological and Biological/Chemical Weapons at the Operational Planning Level.* Department of Operations. Newport: Naval War College.

Grandon, E. E., and Pearson, J. M. (2004). Electronic commerce adoption: An empirical study of small and medium U.S. businesses. *Information & Management, 42*, 197-216.

Groves, R. M. (1989). *Survey Errors and Survey Costs*. New York: Wiley.

Hanney, S., Gonzalez-Block, M., Buxton M., and Kogan M. (2002). *The utilisation of health research in policy-making: concepts, examples and methods of assessment*. A report to the World Health Organization, Health Economics Research Group: Brunel University, Uxbridge.

Harris, R. J. (1993). Multivariate analysis of variance. In L.K.Edwards (Ed.), *Applied Analysis of Variance in Behavioral Science, Statistics Textbooks and Monographs* (pp. 225-296). New York: Marcel Dekker Inc.

Heilig, M. L. (1962). *The original multimedia multisensory virtual reality: Sensorama Stimulator*. United States Patent and Trade Office, Virginia, USA, US-3,050,870.

Henry, G. T. (1990). *Practical Sampling*. Newbury Park, CA: Sage.

Hull, H., Danila, R., and Ehresmann, K. (2003). Smallpox and bioterrorism: Public-health responses. *Journal. Lab. Clin. Med., 142*, (4), 221–228.

Hunt, E. (1991). Some comments on the study of complexity. In R. J. Sternberg and P. A. Frensch (Eds), *Complex Problem Solving: Principles and Mechanisms* (pp. 383-395). Hillsdale, NJ: Lawrence Erlbaum Associates.

Hutchins, E., and B. Hazlehurst (1995). How to invent a lexicon: The development of shared symbols in interaction. In N. Gilbert and R. Conte (eds.) *Artificial societies: The computer simulation of social life* (p. 157-189). UCL Press, London.

Hyacinthe, B. (2004). *Universal Cellular Circuit Board*. United States Patent and Trade Office, VA, US-60/601658035.

Hyacinthe, B. (2005a). *Prevention and Neutralization of Bioactive Substances*. United States Patent and Trade Office, VA. US-60/700708.

Hyacinthe, B. (2005b). *Emergency Rescue Vehicle*. United States Patent and Trade Office, VA., US-60/634,637.

Hyacinthe, B. (2006a). *System and Device for Prevention and Neutralization of Bioactive Substances and Generating an Aroma-producing Substance*. United States Patent and Trade Office, VA., US-60/700,708.

Hyacinthe, B. (2006b). Autonomous Biochemical Decontaminator (ABCD) Against Weapons of Mass Destruction. *Proceedings of SPIE, (6201),* 25, 1-16.

Hyacinthe, B. (2006c). Hidden Global Security Threats and Emerging Technologies Exposed through Information Warfare Paradigms. *Proceedings of the 5th European Conference on Information Warfare and Security*, 101-110.

Hyacinthe, B. (2006d). Methods and Apparatus for the Production of Olfactory and Gustatory Information. *Proceedings of the ACM/JCDL'06*,1-59593-354.

Hyacinthe, B. (2006e). *Apparatus and Methods to Suppress Fluidic Diffusion of Unwanted Substances in Standard Systems, Nano-devices, and Bio-microelectromechanical Systems*. United States Patent and Trade Office, VA., US-60/814320.

Hyacinthe, B., and Anglade, Y. (2007). Conceptual Design of a Microfluidics Suppressor to Protect against Potentially Lethal Printing Devices: A Scenario-Based Physical Cyber Security Measure. *Proceedings of the 2nd International Conference on i-Warfare and Security (ICIW 2007),* 101-110.

Hyacinthe, B., Debbabi, M., Boukhtouta A., Hyatt, Z., Anglade, Y. (2007). Lethal Mutation versus Messianic Singularity: "A New Multidimensional Perspective on the Reciprocal Function of Digital Information Technologies as Offensive and Defensive Weapon Systems." *6th European Conference on Information Warfare and Security Defence*, Defence Academy of the United Kingdom, Shrivenham, UK, pp.99-108.

Igbaria, M., Parasuraman, S., and Baroudi, J.J. (1996). A Motivational Model of Microcomputer Usage. *Journal of Management Information Systems, 13*(1), 127-143.

Ingwersen, P. (1996). Cognitive Perspectives of Information Retrieval Interaction: Elements of a Cognitive IR Theory. *Journal of Documentation, 52*(1), 3-50.

Ishida, H., Nakamoto, T., and Moriizumi, T. (1996). Study of odor compass. *Proceedings of Int. Conf. on Multi-sensor Fusion and Integration for Intelligent Systems*, 222-226.

Jackson, C. M., Chow, S., and Leitch, R. A. (1997). Toward an understanding of the behavioral intention to use an information system. *Decision Sciences, 28*(2), 357-389.

Jaeger, P. (2005). *Multi-method evaluation of U.S. Federal Electronic Government Websites in Terms of Accessibility for Persons with Disabilities*. (PhD Thesis). Florida: Florida State University.

Jankowski, P., Mercado, A., Hallowell, S. (1992). FAA explosive vapor/particle detection technology. *Proceedings of SPIE (1824),* 13-24.

Johnson-Laird, P. (1983). *Mental Models*. Cambridge: Harvard University Press.

Kanzaki, K., Nagasawa, S., and Shimoyama, I. (2005). Neural Basis of Odor-source searching behavior in insect brain systems evaluated with a mobile robot. *Chemical Senses, 30*, i285-i286.

Kaplan, B., and Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: A case study*. MIS Quarterly, 12* (4), 571-586.

Karahanna, E., and Straub, D.W. (1998). The psychological origins of perceived usefulness and ease-of-use. *Information and Management, 35*, 237-250.

Keil, M., Beranek, P.M., and Konsynski, B.R. (1995). Usefulness and Ease of Use: Field Study Evidence Regarding Task Considerations. *Decision Support Systems, 13*(3), 75-91.

Kelman, H. C. (1958). Compliance, Identification, and Internalization: Three processes of Attitude Change? *Journal of Conflict Resolution, 2*, 51-60.

Kiesler, S. (1997). *The Culture of the Internet*. Mahwah, NJ: Lawrence Erlbaum Associates.

Kim, S., and Malhotra, N. (2005). A longitudinal model of continued IS use: An integrative view of four mechanisms underlying post adoption phenomena. *Management Science, 51*(5), 741-755.

Kling, R. (2000). Learning about information technologies and social change: The contribution of social informatics. *The Information Society, 16*(3), 217-232.

Kling, R., Rosenbaum, H., and Hert, C. (1998). Social Informatics in Information Science: An Introduction. *Journal of the American Society for Information Science, 49*(12), 1047-1052.

Kock, N., McQueen, R., and Scott, J. (1997). Can action research be made more rigorous in a positivist sense? *The contribution of an iterative approach. Journal of Systems and Information Technology, 1*(1), 1-24.

Kosslyn, S. M., and Sussman, A. L. (1995). Roles of imagery in perception: Or, there is no such thing as immaculate perception. In M. S. Gazzaniga (Ed.), *The cognitive neurosciences* (pp.1035–1042). Cambridge, MA: MIT Press.

Kosslyn, S., Ball, T., and Reiser, B. (1978). Visual images preserve metric spatial information: evidence from studies of image scanning. *Journal of Experimental Psychology: Human Perception and Performance, 4*, 47–60.

Kuhlthau, C. (1994). *Seeking meaning: a process approach to library and information services*. Norwood, NJ., Ablex Publishing.

Kuhlthau, C. (1991). Inside the Search Process: Information Seeking from theUser's Perspective. *Journal of the American Society for Information Science 42*(5), 257-304.

Labaw, P. J., (1980). *Advanced Questionnaire Design*. Cambridge, MA: Abt Books.

Larkin, J.., and Simon, H. (1987). Why a diagram is (sometimes) worth ten thousand words. *Cogn Sci., 11*, 65–99.

Latham, R. (2003). *Bombs and bandwidth: The emerging relationship between information technology and security*. New York: The New Press.

Lau, F. (1997). A review on the use of action research in information systems studies. In Lee, A.S., Liebenau, J., and DeGross, J.I. (Eds), *Information systems and qualitative research* (pp. 31-68). London: Chapman and Hall, London.

Lavis, J., Ross S, McLeod C, Gildiner A. (2003). Measuring the impact of health research. *Journal of Health Services Research & Policy, 8*,165-70.

Lazzaro, J. (1989). *Silicon Models of Early Audition. Computer Science, California Institute of Technology*. Caltech Computer Science Technical Report Caltech (PhD Thesis). California: CS-TR-89-10.

Lazzaro, J. P. (1991). Biologically-based auditory signal processing in analog VLSI. *IEEE Asilomar Conference on Signals, Systems, and Computers*, 790-794.

Lazzaro, J. P. (1992). Temporal adaptation in a silicon auditory nerve. In Moody, J., Hanson, S., Lippmann, R. (eds), *Advances in Neural Information Processing Systems* (p.p. 813-820). San Mateo, CA: Morgan Kaufmann Publishers.

Lederer, A. L., Maupin, D. J., Sena, M. P., and Zhuang, Y. (2000). The technology acceptance model and the World Wide Web. *Decision Support Systems, 29*(3), 269-282.

Lee, C. (2003). *Fragrance emitter for use with Internet*. United States Patent and Trademark Office, Washington, DC., US-6524537.

Le Gac, S., Rolando, C., Druon, C., and Tabourier, P. (2002). Systèmes microfluidiques intégrés pour l'analyse et l'étude de la réactivité chimique. *Proceedings of NTC*, Rennes, France.

Le Gac, S., Rolando, C., Druon, C., Tabourier, P., Lefèbvre, P., and Mélique, X. (2001). On-chip chromatography column for biological sample purification and concentration. *Proceedings on Microreaction Technology*, Montréal, Canada.

Le Gac, S., Rolando., C., Arscott, S., Carlier, J., Caron, F., Fourrier, J., Thomy, V., Druon, C., Tabourier, P., and Camart, J. (2003). Microfluidics for proteomics: discrete liquids. *Japan-European Workshop on Chem Micro Mechatronics Systems and Biochips*, ENS Cachan.

Legris, P., Ingham, J., and Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information and Management, 40* (3), 191-204.

Libicki, M. (1995). What is Information Warfare Strategic. *Forum, (5)*28, 1-104.

Lin, C. J., and Lu, H. (2001). Towards an understanding of the behavioral intention to use a web site. *International Journal of Information Management, 20*, 197-208.

Littleton, M. (2005*). Information age terrorism: Toward Cyberterror*. Available: http://www.fas.org/irp/threat/cyber/docs/npgs/terror.htm#note1.

Loewenstein, W. R. (1999). *Molecular information, cell communication, and the foundations of life*. New York: Oxford University Press.

Luarn, P., and Lin, H. (2005). Toward an understanding of the behavioral intention to use mobile banking. *Computers in Human Behavior, 21*(6), 873-891.

Lucas, H., and Spitler, V. K. (1999). Technology use and performance: A field study of broker workstations. *Decision Sciences*, *30*(2), 291-311.

Machlup, F., Mansfield, U. (Eds.) (1983). *The Study of Information. Interdisciplinary Messages.* New York: Wiley.

Maes, P. (1994). Agents that reduce work and information overload. *CACM*, *37*, 7, 30-40.

Malcolm, D. (2001). Genomics and Future Biological Weapons: The Need for Preventative Action by the Biomedical Community. *Nature Genetics, 29*, 253-265.

Manne, J. (1999). *Multimedia linked scent delivery system*. United States Patent and Trade Office, Washington, DC. US5949522.

Marijuan, P.C. (1996). First conference on foundations of information science. From computers and quantum physics to cells, nervous systems, and societies. *Bio Systems 38*, 87-96.

Markus, L. (1987). Toward a 'critical mass' theory of interactive media: Universal access, interdependence and diffusion. *Communication Research, 14*, 491–511.

Markus, M., and Bjorn-Anderson, N. (1987). Power Over Users: It's Exercise by System Professionals. *Communications of the ACM*, *30*(6), 498-502.

Marques, L., De Almeida, A.T. (2000). Electronic nose-based odour source localization. *Proceedings. 6th International Workshop on Advanced Motion Control,* 36-40.

Martin, P., and Bateson, P. (1986). *Measuring Behavior: An Introductory Guide*. Cambridge: Cambridge Univ. Press.

Martins, L., and Kellermanns, F. (2001). User acceptance of a web-based information system in a non-voluntary context. *22nd ICIS Conference*, 607-612.

Mayzner, M., and Dolan, T. (1978). *Minicomputers in Sensory and Information-Processing Research*. Lawrence Erlbaum Associates. Hillsdale, New Jersey.

McCoy, T. (1999). *Issues in Civilian Disaster Planning and Management For Incidents of Chemical and Biological Terrorism* (Military Thesis). Houston, TX: Academy of Health Sciences, Army.

McCoy, S., Everard, A., and Jones, B. M. (2005). An examination of the technology acceptance model in Uruguay and the US: A focus on culture. *Journal of Global Information Technology Management*, *8*(2), 27-45.

McCulloch, W., and Pitts, W. (1965). A Logical Calculus of the Ideas Immanent in Nervous activity. In W.S. McCulloch (Ed.), *Embodiments of Mind* (pp.19-39). Cambridge, Massachusetts: The MIT Press.

McFarland, D.J., and Hamilton, D. (2006). Adding contextual specificity to the technology acceptance model. *Computers in Human Behavior, 22*(3), 427-447.

Mead, C. A., Arreguit, X., and Lazzaro, J. P. (1991). Analog VLSI models of binaural hearing. *IEEE Journal of Neural Networks 2*, 230-236.

Melone, N. P. (1990). A Theoretical Assessment of the User Satisfaction Construct in Information Systems Research. *Management Science, 36*, 76-91.

Miles, M., and Huberman, A. (1984).*Qualitative data analysis*. London: Sage.

Miller, G.A. (1956). The Magical Number Seven, Plus or Minus Two: some limits on our capacity for processing information. *Psychological Review, 63*, 81-97.

Mingers, J., and Gill, A. (1997). *Multimethodology: the Theory and Practice of Combining Management Science Methodologies*. John Wiley, Chichester, UK.

Miwa, H., Umetsu, T., Takanishi, A., and Takanohu, H. (2001). Human-like robot head that has olfactory sensation and facial color expression. *IEEE International Conference on Robotics and Automation,1*, 459- 464.

Molander, R., Riddile, A., and Wilson, P. (1996). *Strategic information warfare: A new face of war*. Santa Monica, CA: RAND.

Morgan, P. (2003). Information Warfare and Domestic Threats to America Security. *Contemporary Security Policy, 24*,161-189.

Morse, J. (2003). Principles of mixed and multi-method research design. In A. Tashakkori. and C. Teddlie (Eds.), *Handbook of mixed methods in social and behavioral research* (pp.189-208). London: Sage Publications.

Mueller, P., and Lazzaro J. (1986). A machine for neural computation of acoustical patterns with applications to real-time speech recognition. In Denker, J. (Ed.), *Neural Networks for Computing* (pp. 321-327). Utah: Snowbird.

Mukherjee, G., and Fedder, T. (1998). Design methodology for mixed-domain systems-on-a-chip [MEMS design]. *Proc. IEEE VLSI System Level Design*, 96 – 101.

Murray, J. (1997). *Hamlet on the Holodeck; The Future of Narrative in Cyberspace*. Cambridge, Massachusetts: MIT Press.

Ndubisi, N. O., and Jantan, M. (2003). Evaluating IS usage in Malaysian small and medium-sized firms using the technology acceptance model. *Logistics Information Management, 16*(6), 440-450.

Nelson, K., Paulsen, J., Heldelberg, J., and Fraser, C. (2000). Status of genome projects for nonpathogenic bacteria and archea. *Nature Biology, 18*, 1049-1054.

Nobre, A. C., Coull, J. T., Maquet, P., Frith, C. D., Vandenberghe, R., and Mesulam, M. M. (2004). Orienting attention to locations in perceptual versus mental representations. *Journal of Cognitive Neuroscience, 16 (3),* 363–373.

O'Neil, S. (2006). *Lockheed Martin to design nano air vehicle to monitor the urban battlefield*. Available: http://www.lockheedmartin.com/.

Ostrom, T. (1988). Computer simulation: the third symbol system. *Journal of Experimental Social Psychology, 24, 381-392.*

Paivio, A. (1971). *Imagery & Verbal Processes*. New York: Holt & Co.

Paradies, C., and Hyacinthe, B. (2005). *Patent Search on computer-related olfactory systems*. Law Offices of White, Boggs and Fowler. Tampa, Florida.

Patels, H.R. (1988). *The Dreams of Reason*. New York: Banta.

Preliminary British Intelligence Report. (2006). *Radiation found after spy's death*. Available: http://news.bbc.co.uk/2/hi/uk_news/6180682.stm

Quinn, D.M., Balasubramanian, A.S., Doctor B.P., and Taylor, P. (1995). *Enzymes of the Cholinesterase Family*. New York: Plenum Press.

Raber, D. (2003). *The problem of information: An introduction to information science*. The Scarecrow Press, Lanhand, Maryland.

Radić, Z., Reiner E., and Taylor P. (1991). Role of the peripheral anionic site on acetylcholinesterase: inhibition by substrates and coumarin derivatives. *Molec Pharmacol. 39*, 98-104.

Radnedge, L., Gamez-Chin, S., McCready, P., Worsham, P., and Andersen, G. (2001). Identification of nucleotide sequences for the specific and rapid detection of Yersinia pestis*. Appl. and Env. Microbio., 67*, 3759-3762.

Ramnath, K.C., and Pavlou, A. P. (2002). Perceived information security, financial liability and consumer trust in electronic commerce transactions. *Logistics Information Management, 15*(5/6), 358-368.

Rasouli, F., Arastoopour, H., and Oskouie, A. (1999). *Apparatus for generating odor upon electronic signal demand*. United States Patent and Trademark Office, Washington, DC. US-6004516.

Reiner E., and Radić Z. (2000). Mechanism of action of cholinesterase inhibitors. In E. Giacobini (Ed.), *Cholinesterases and Cholinesterase Inhibitors* (pp. 103-119). Martin Dunitz Ltd., London.

Renaudin, A., Zhang, V., Tabourier, P., Camart, J., and Druon, C. (2004). Droplet manipulation using SAW actuation for integrated microfluidics, *µTAS*, Malmö, Sweden.

Ringland, G. (1998*). Scenario planning: Managing for the future*. New York: John Wiley.

Robey, D., and Farrow, D. (1982). User Involvement in Information System Development: A Model and Empical Test. *Management Science, 28*, 1, 73-85.

Rogers, E. (1995). *Diffusion of Innovations*. The Free Press, NY.

Rogers, E.M. (1976). New product adoption and diffusion. *The Journal of Consumer Research, 2*(4), 290-301.

Rosnow, R., and Rosenthal, R. (1996). *Beginning Behavioral Research: A Conceptual Primer (Ed.)*. Prentice-Hall. Englewood Cliffs, NJ.

Russell, L., Berberich, J., Drevon, G., and Koepsel, R. (2003). Biomaterials for mediation of chemical and biological warfare agents. *Annual Review of Biomedical Engineering 3*, 5, 1-27.

Russell, R.A., and Purnamadjaja, A.H. (2002). Odor and airflow: complementary senses for a humanoid robot. *Proc. Robotics and Automation, IEEE International Conference, 2*, 1842-1847.

Salant, P., and Dillman, D. (1994). *How to Conduct Your Own Survey*. New York: Wiley.

Saracevic, T. (1999). Information Science. *JASIS, 50* (12): pp.1051-1063.

Satzinger, J.W., and Olfman, L. (1995). Computer Support for Group Work: Perceptions of the Usefulness of Support Scenarios and End-User Tools. *Journal of Management Information Systems, 11*, (4), 115-148.

Schewe, C. (1976). The management Information System User: An Exploratory Behavioral Analysis. *Academy of Management Journal, 19*, 4, 577-590.

Schneiderman, B. (1997). *Designing the User Interface*. Addison Wesley, MA.

Schrader, A. (1984). In Search of Search: Informational Science and Its Conceptual Antecedents. *Library and Information Science Research, 6*, 227-271.

Schultz, R., and Slevin, D. (1975). *Implementation and Organizational Validity: An empirical Investigation in Implementing Operation Research/Management Science*. American Elsevier, New York, NY.

Schwartz, P. (1991). *The Art of the Long View*. New York: Doubleday.

Shannon, C.E., and Weaver, W. (1949). *The Mathematical Theory of Communication*. Urbana, University of Illinois Press.

Shannon, C.E. (1949). Communication theory of secrecy systems. *Bell Systems Technical Journal, 28,* 656-715.

Sharma, S., and Gupta, J. (2002). Securing information infrastructure from information warfare. *Logistics Information Management, 15*, 414-422.

Shneiderman, B. (1980). *Software Psychology: Human Factors in Computer and Information Systems*. Cambridge, MA: Winthrop.

Short, J., Williams, E., and Christie, B. (1976). *The Social Psychology of Telecommunications*. Wiley, NY.

Singh, S., and Singh, M. (2003). Explosives detection systems (EDS) for aviation security. *Signal Processing, 83*, 31-55.

Soulliere, D., Britt, D., Maines, D. (2001). Conceptual Modeling as a Toolbox for Grounded Theorists. *Sociological Quarterly 42*(2), 253–69.

Spacey, R., Goulding, A., and Murray, I. (2004). Exploring the attitudes of public library staff to the internet using the TAM. *Journal of Documentation, 60*(5), 550-564.

Sperberg-McQueen, C., Huitfeldt, M., and Renear, A. (2000). Meaning and Interpretation of Markup. *Markup Languages: Theory & Practice 2*(3), 215-234.

Srinivasan, V., Pamula, V., Pollack., Fair, R.(2003). A digital microfluidic biosensor for multianalyte detection. *Proceedings of the IEEE 16th Annual International Conference on Micro Electro Mechanical Systems*, 327-330.

Srinivasan, V., Pamula, V., and Fair, R. (2004). An Integrated Digital Microfluidic Lab-on-a-chip for Clinical Diagnostics on Human Physiological Fluids. *Lab on a Chip, 4*, 265-277.

Straub, D., Keil, M., and Brenner, W. (1997). Testing the technology acceptance model across cultures: a three country study. *Information and Management, 33*, 1-11.

Strauss, A. L., and Corbin, J (1990). *Basics of qualitative research: grounded theory procedures and techniques*. Newbury Park, CA: Sage Publications.

Stuckey-French, N. (2001). *Bioterror-Then and Now*. Available: http://www.inthesetimes.com/issue/25/26/feature4.shtml

Suh, B., and Han, I. (2003). The Impact of Consumer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. *International Journal of Electronic Commerce, 7*, 3,135-161.

Sutton, V., and Bromley, D. (2005). Understanding technologies of terror. *Technology in Society, 27*, 263-285.

Swanson, E. (1974). Management Information Systems: Appreciation and Involvement. *Management Science, 21*, 2, 178-188.

Szajna, B. (1996). Empirical evaluation of the revised technology acceptance model. *Management Science, 42*(1), 85-92.

Taylor, K. (1990). *An Expert System To Assist Design*. (PhD Thesis). Nottingham: University of Nottingham.

Taylor, S., and Todd, P. (1995). Understanding Information Technology Usage: A Test of Competing Models. *Information Systems Research, 6*(2), 144-176.

The 9/11 Commission Report. (2004). *9/11 Commission Report: Final Report of the National Commission on Terrorism Attacks Upon the United States*. Available: http://www.gpoaccess.gov/911/

Toffler, A., and Toffler, H. (1993). War *and Antiwar: Survival at the Dawn of the 21st Century*. Boston: Brown & Co.

Tornatzky, L., and Fleischer, M. (1990). *The Process of Technological Innovation*. New York: Pergamon Press.

Torrens, L. (1999). *Conflict in the 21st Century: Counterstrategies For the WMD Terrorist*. Maxwell Air Force Base. Alabama: Air University.

Valentine, M., Perlman, Z., Gardel, M., Shin, J., Matsudaira, P., Mitchison, T., and Weitz, D. (2004). Colloid Surface Chemistry Critically Affects Multiple Particle Tracking Measurements of Biomaterials. *Biophysical Journal, 86*, 6, 4004–4014.

Van der Heijden, K., Bradfield, R., Burt, G., Cairns, G., and Wright, G. (2002). *The sixth sense: Accelerating organizational learning with scenarios*. New York: John Wiley.

Van der Heijden, H., Tibert, V., and Creemers, M. (2003). Understanding online purchase intentions: Contributions from technology and trust perspectives. *European Journal of Information Systems, 12(*1), 41.

Venkatesh, S., and Memish, Z. (2003). Bioterrorism: A new challenge for public health. *Int. J. Antimicrob. Agent, 21*, 2, 200–206.

Venkatesh, V. (2000). Determinants of perceived ease of use: Integrating control, intrinsic motivation, emotion into the technology acceptance model. *Information Systems Research, 11* (4), 342-365.

Venkatesh, V., and Davis, F. D. (1996). A model of the antecedents of perceived ease of use: Development and test. *Decision Sciences, 27*(3), 451-481.

Venkatesh, V., and Davis, F.D. (2000). A theoretical extension of the TAM: Four longitudinal field studies. *Management Science, 46*(2), 186-204.

Venkatesh, V., and Morris, M.G. (2000). Why don't men ever stop to ask for directions? Gender, social influence, and their role in technology acceptance and usage behavior. *MIS Quarterly, 24* (1), 115-39.

Vijayasarathy, L.R. (2004). Predicting Consumer Intentions to Use Online Shopping: The Case for an Augmented Technology Acceptance Model. *Information & Management, 41* (6), 747-762.

Wang, H., Tsai, Y., and Wu, F. (2004). *Information apparatus with interactive scent interface*. United States Patent and Trademark Office. Washington, DC. US-2004024043.

Wang, W., and Benbasat, I. (2005). Trust in and Adoption of Online Recommendation Agents. *Journal of the Association for Information Systems, 6*(3), 72-101.

Wasserman, S., and Faust, K. (1994). *Social Network Analysis*. Cambridge, MA: Cambridge University Press.

Waters, D. (2007). *Technology 'embraced by public.'* Available: http://news.bbc.co.uk/1/hi/technology/6238309.stm

Watson, M. (1997). *Intelligent Java Applications for the Internet and Intranets*. San Francisco, CA: Morgan Kaufmann Publishers Inc.

Webb, D. (1999).*The Prospects For International Terrorist Groups Employing Chemical Weapon* (Military Thesis). Maxwell Air Force Base, AL: Air University.

Weber, R. P. (1985). *Basic Content Analysis*. Beverly Hills, CA: Sage.

Weiss, CB. (1979). The many meanings of research utilization. *Public Administration Review, 39*, 426-31.

Wiener, N. (1948). *Cybernetics, or control and communication in the animal and the machine*. Cambridge, Massachusetts: The Technology Press. New York: John Wiley & Sons.

Wilson, T. D. (1981). On User Studies and Information Needs. *Journal of Documentation, 37*(1), 3-15.

Wilson, T. D. (1984). The Cognitive Approach to Information-Seeking Behavior and information Use. *Social Science Information Studies 4*(2), 3: 197-204.

Wilson, T. D. (1999). Models in information behaviour research. *Journal of Documentation, 55*(3), 249-270.

Winkin, Y. (2003). L'haleine de la ville : la sémiologie olfactive de Simenon. In J-L Dumortier (Ed.), *Le Roman de Simenon. Pedigree : entre réalité et fiction* (pp. 243-250). Brussels.

Wisneski, C. A. (1999). *The Design of Personal Ambient Displays* (Master's Thesis). Massachusetts: Massachusetts Institute of Technology.

Yin, R. (1984). *Case Study Research: Design and Methods*. Beverly Hills: Sage.

Yoong, P., and Pauleen, D. (2004). Generating and analyzing data for applied research on emerging technologies: a grounded action learning approach. *Information Research, 9*, 4(7). Available: http://informationr.net/ir/9-4/paper195.html

Zhang, T., Chakrabarty, K., and Fair, R. (2002). *Microelectrofluidic Systems: Modeling and Simulation*. Boca Raton, Florida: CRC Press.

BIOGRAPHICAL SKETCH

Berg P. Hyacinthe

My main objective is to invent, design, and develop emergent technologies under a cyber-conditioning paradigm of consumer electronics and to secure and protect critical information infrastructures against hidden and future threats. My research interests encompass: Emerging Technologies, Information Warfare, Social Informatics, and Cyber-Assisted Olfactory Communication.

EDUCATION

Florida State University Tallahassee, FL
PhD. (Candidate)

Florida Gulf Coast University Fort Myers, FL
Master's Degree: Educational Technology

Florida State University Tallahassee, FL
Bachelor's Degree: Bachelor of Art "with honors"

Edison College Fort Myers, FL
Computer Science Associate Degrees (Programming and Applications – AS&AA)

Sony Electronics Training Center Fort Myers, FL
Certified Computer Technician (Computers and Electronics)

Languages: Fully bilingual (English and French)

The International Society for Optical Engineering (SPIE)
Golden Key Honor Society

EXPERIENCE

Infosense Technologies and Research, Sunrise, FL
Researcher

- Investigate threats associated with aroma-embedded information systems
- Develop protocols for an autonomous biochemical decontaminator
- Identify hidden threats associated with information systems
- Develop advanced physical cyber security protocols
- Explore bio-microelectromechanical systems as countermeasures

Florida State University Tallahassee, FL
Doctoral Student – Teaching Assistant

- Maintain teaching protocols for Interface Design class (LIS4351)
- Assist students in developing Web applications (Java)
- Provide leadership and advanced support to students
- Supervise group of computer programmers, lecture , and grade assignments

Collier County Government, Naples, FL
IT Professional

- Serve as IT Consultant to the Board of County Commissioners
- Serve as an account manager for the division of Administrative Service
- Assist in Web initiatives (E-Government, Cyber-Training, and Internet Policies and Security). Advise on acquisition of IT resources countywide
- SAP, Crystal Report, MS Project, Visio, and other customized databases

Florida Gulf Coast University, Fort Myers, FL
IT Computer Specialist

- Assist faculty and staff in critical IT decisions
- Provide expertise and recommendations in designing IT master plan
- Provide assistance in the delivery of distance learning courses (Web)
- Utilize SPSS and Crystal Report as management tools

INTERESTS

Invent and innovate through the introduction of revolutionary emergent technologies with applications in various sectors to include consumer electronics, biomedical engineering, and defense and security.

Develop robust security protocols for the emerging aroma-embedded information systems through a new approach to Microfluidics and bio-micro electromechanical systems.

Secure new concepts and novel technologies via intellectual property licenses, patents, and collaborations with other leading scientists that are likely to contribute to timely technology transfer from *design* to *prototype* to *fabrication*. I have a special interest in hardware security.

PUBLICATIONS

Published Articles

Hyacinthe *et al.* (2007). Lethal Mutation versus Messianic Singularity: "A New Multidimensional Perspective on the Reciprocal Function of Digital Information Technologies as Offensive and Defensive Weapon Systems." *6th European Conference on Information Warfare and Security Defence*, Defence Academy of the United Kingdom, Shrivenham, UK, pp.99-108.

Hyacinthe, B. and Anglade, Y. (2007). Conceptual Design of a Microfluidics Suppressor to Protect against Potentially Lethal Printing Devices: A Scenario-Based Physical Cyber Security Measure. *ICIW 2007: 2nd International Conference on i-Warfare and Security*, U.S. Naval Postgraduate School, Monterey, California. pp. 101-110.

Hyacinthe, B. (2006). Autonomous Biochemical Decontaminator (ABCD) against Weapons of Mass Destruction. *SPIE*, vol. 6021:1-16. Orlando, USA.

Hyacinthe, B. (2006). Hidden Global Security Threats and Emerging Technologies Exposed through Information Warfare Paradigms. *Proc. of the 5th European Conference on Information Warfare and Security*, Helsinki, Finland. pp. 101-110.

Hyacinthe, B. (2006). Methods and Apparatus for the Production of Aromatic and Gustatory Information. *JDCL*, Chapel Hill, NC. ACM 1-59593-354-9.

Published Patents

Hyacinthe, B. (2006). *System and Device for Prevention and Neutralization of Bioactive Substances and Generating an Aroma-producing Substance*. USPTO.VA. US-60/700,708.

Hyacinthe, B. (2005). *Universal Cellular Circuit Board*. USPTO. VA. US-60/601658035.

Hyacinthe, B. (2004). *Emergency Rescue Vehicle*. USPTO. VA. US-60/634,637.

Provisional Patent Applications

Hyacinthe, B. (2006). *Apparatus and Methods to Suppress Fluidic Diffusion of Unwanted Substances in Standard Systems, Nano-devices, and Bio-microelectromechanical Systems*. USPTO. VA. US-60/814320.