Professional Ethics Report
Current Issue — PER Main Page — SFRCL Main Page

Volume XI, Number 4, Fall 1998

Publication of the AAAS Scientific Freedom, Responsibility and Law Program, in collaboration with the Committee on Scientific Freedom and Responsibility
Professional Society Ethics Group
Editor: Mark S. Frankel
Deputy/Managing Editor: Sanyin Siang
Contributing Editors: Emily Feinstein, Michele Garfinkel, Rachel Gray, Bhavani Pathak, Nick Williamson
ISSN: 1045-8808
URL: http://www.aaas.org/spp/sfrl/sfrl.htm

The Legitimization of Strategic Information Warfare: Ethical Considerations

By Roger C. Molander and Sanyin Siang

Roger C. Molander is a senior research scientist at RAND. Sanyin Siang is Deputy Editor of Professional Ethics Report.

The development of the Internet and the Web has resulted in a global society dependent on information technology. As a consequence, there emerges profound problems of scientific ethics and international security that have been increasingly drawing the attention of international security experts, especially those concerned about the future of strategic warfare. Call it cyberwar or strategic information warfare (SIW).

Many countries rely on information-based resources, including management systems and infrastructures involving the control of electric power, money flow, air traffic, and other information-dependent items. SIW occurs when one national seeks to obtain strategic leverage over another by severely disrupting or damage these systems by exploiting the tools and techniques of the Internet. Compared to other strategic forms of warfare such as nuclear war or the clash of massed armies, SIW possesses several distinct features. The entry cost is potentially much lower. There is difficulty in ascertaining perpetrator identity, thereby, enhancing opportunities for deceptive attackers. It also generates new tactical warning and attack assessment problems since there is currently no adequate means for distinguishing between SIW attacks and other kinds of cyberspace activities, including espionage or accidents. Furthermore, in the world of SIW, there is no frontline; the “battlegrounds” are everywhere, from the stock market to the natural gas pipelines. In short, the expanding global network and its rise as a new mode of communication, transcends physical space, thereby muddying the geographical boundaries and traditional distinctions between the public and the private, the criminal and the warlike, the civilian and the military. Lastly, SIW seems to possess the redeeming quality of being “much more humane” than other forms of strategic warfare since the only intended casualties would be the crippling of information flow, convenience, and comfort.

An understanding and development of this technology can lead to great strides in attack capabilities. The question remains whether SIW should be legitimized as a new form of warfare. To explore this question, we will examine the ethical considerations in terms of offensive and defensive capabilities.

For the past several years, a comprehensive understanding of the impact of cyberwarfare has eluded the international security community. It is too early in its inception to determine the full extent to which someone might develop and use the capability to hack a critical infrastructure to pieces and maybe refuse to admit to the act. All nations see a need for new intelligence assessment and analysis methods to deal with this emerging threat. The absence of technology that permits identification of the cyber attacker with absolute certainty makes nations especially susceptible to a new kind of manipulation. For example, a terrorist group intent on provoking war between the U.S. and China, can carry out a cyber attack which deceives the U.S. into thinking the culprit to be China. Faced with such possibilities, reliance on any kind of deterrence strategy that assumes an ability to unambiguously identify an attacker seems unpromising. At the same time, owners and operators of critical infrastructures must assess their vulnerabilities to threats from

cyberspace, from both nations and terrorists.

Of even greater concern is the emergence of cyberspace attack as the critical ingredient in a new witches brew of strategic warfare capability. Consider the prospect of a carefully constructed strategic warfare campaign seeking to achieve the strategic leverage of effecting mass disruption though combined attacks on key infrastructure nodes and other infrastructure targets via conventional means, via new unconventional means (e.g., electromagnetic weapons), and via information warfare tools and techniques. Such a capability poses a wholly new kind of threat to international stability.

Looking back before looking forward on this matter, the path followed from the development of the ARPANET through the emergence of the hacking community and culture, in parallel with ever evolving tools and techniques of electronic warfare for military ends, seems understandable enough. But the consequences of this path, and the larger implications for society and the future of warfare are only now beginning to reach national and international consciousness. Moreover, this consciousness has emerged in a wholly new international security environment marked by the end of the Cold War and the long shadows cast by the 1991 Persian Gulf War.

In the former case, strategic thinkers in the international security arena are pondering the future of strategic warfare, with great emphasis in the near term (absent a global peer competitor to the United States) on the character of strategic warfare at the regional level, e.g., in the Middle East or Northeast Asia. The Gulf War provided a clear lesson learned for all would–be regional hegemons: Don't take on the U.S. and its allies on a traditional conventional battlefield. There other approaches, other means and strategies, for regional powers to take on such powerful coalitions – so-called asymmetric strategies such as those involving the use of biological or chemical weapons to counter an attack. In other words, SIW offers a new element of strategy for adversaries of nations like the US and its allies to consider.

Another complexity introduced by the potential for SIW is that some nations may develop SIW capabilities and hope that attacks with such weapons will only face repsonses in kind. However, there is no guarantee that an adversary nation will feel limited to an SIW response, especially if it has other instruments of strategic information warfare readily available.

This scenario also illustrates the unpredictability of using SIW. Envision a nation developing - and implementing through brandishing or actual use - a capability to disrupt the delivery of services from critical infrastructures. Try further, in a fast moving Information technology (IT)-driven environment, to envision that those who would offer such tools and techniques of strategic warfare - or terrorism - to decision-makers would be able to forecast accurately the collateral effects and overall consequences of an attack of any strategic magnitude. The first is readily conceivable; the second is almost inconceivable. No further examples are needed than those already on the record of the prospect of profound unforeseen cascading consequences of disruptions caused by innocent acts such as the 1997 falling tree incident in Wyoming, which had far-ranging negative impact on electrical service delivery as far away as southern California. In the light of such realities, can one possibly envision that the true consequences of a strategic campaign based in large measure on infrastructure attack via cyberspace can possibly be predicted?

It is not hard to construct very sobering scenarios in the light of these considerations. A supposedly limited precision attack on a segment of an electric power grid could have the unintended consequences of widespread power outages and the failure of emergency power services at places like hospitals and other critical facilities. Or a modest but widespread attack could simply produce far larger consequences across the board due to poorly understood infrastructure interdependencies (e.g., between electric power and telecommunications) and catalyze an unexpectedly larger response and conflict escalation. Thus, given continued poor understanding of infrastructure interdependencies, can SIW attacks under such "imprecisions" be justifiable? The situation is exacerbated by ethical considerations born of the blurred distinction between the public and the private. In cyberwar, the frontline is no longer defined by the military; disruption of the civilian sector may be the explicit objective. In such circumstances, what is "acceptable" and "fair" within the ethics of war as currently judged by civilization?

The search for answers needs to include fostering a serious and far-reaching dialogue on this subject within the international community. In November 1998, a committee of the United Nations General Assembly drafted a final resolution to address this issue. It called upon Member States to "promote the consideration of existing and potential

threats in the field of information security" and invited them to help develop "international principles that would enhance information security and combat information terrorism and criminality." Furthermore, the UN plans to include an item on developments in the field of information security on the agenda for its next session.

The dire character of the above descriptions is not intended to foster a feeling of hopelessness about the infrastructure protection challenge, but rather to stimulate a deeper consideration of the kind of problem that is emerging. Unlike the asymptotic U.S.-Soviet response to the nuclear threat – deterrence largely achieved through the threat of mutual assured destruction – there is relatively little hope that even in the long term the perpetrator identification problem (key to any deterrent concept) can be solved to the unambiguous degree that decision-makers will demand in considering a retaliatory response.

In such emerging circumstances, there appears to be only one strategic response – protection to the degree possible, and rapid response to restore services when protection fails. But can such a national and international strategic response succeed in an environment where the hacker culture – in no small measure the spokesperson for a large segment of the IT community - insists on perpetuating the concept that the breaking down of the defenses of computer networks is an unalloyed good? Is it not far more preferable for the IT community to unanimously embrace the alternative of very quietly helping to fix vulnerability problems when they are discovered?

Furthermore, can the IT scientific and technological community (unable to muster the leadership to acknowledge the Y2K problem years ago, and collectively take steps to remedy it) take a lead role in addressing on an urgent time scale the infrastructure vulnerability problem? While the prospect is not encouraging, the demand is of such a character that it becomes quite literally an ethical issue for the IT community. In the race to reap the financial rewards of the IT revolution, should not those in the scientific and technological communities who gave us the Internet and the Web not take some responsibility here? And should that responsibility not go so far as to change fundamentally the prevailing culture in the hacker community and quite literally turn it around? Should not those who once worked at opening every door now be encouraged - through example and leadership - to take on the task of making cyberspace more secure?

Without such a commitment, the IT community could run the risk that the grand potential of the IT revolution could be profoundly blunted by recurring problems of infrastructure disruption. While there is probably not the danger of the technological "simplification" that followed World War III in William Miller's famous *A Canticle for Liebowitz*, there is a danger that much of the good that can be achieved from the IT revolution will be slower in coming and in the end less far less far reaching than the unalloyed bright shining path that the IT community would now cast before us. Perhaps, better a new ethic that eschews the evolution of cyberspace into a new battlespace.

IN THE NEWS

INTERVIEW TRANSCRIPTS WILL REMAIN CONFIDENTIAL

U.S. District Court Judge Richard Stearns ruled that David B. Yoffie, a professor at Harvard Business School, and Michael A. Cusumano, a professor at Massachusetts Institute of Technology's Sloan School of Management, do not have to turn over interview notes, recordings, and confidential correspondence to Microsoft Corporation. In May 1998, the Department of Justice sued Microsoft, charging that it violated antitrust laws by unfairly using its monopoly in operating system software for personal computers. The trial focuses on Microsoft's allegedly unfair competition with Netscape Communications Corporation, a pioneer in browsers for accessing the Web. Professors Yoffie and Cusumano became involved in the case after authoring a new book, Competing on Internet Time: Lessons from Netscape and its Battle with Microsoft (Free Press), which describes past business practices of Netscape.

Microsoft sought to have access to the professors accumulated research notes and transcripts of 60-70 hours of interview tapes with Netscape executives. According to Microsoft, the interviews would allegedly show that Netscape's own errors in management, and not unfair practices by Microsoft, as the government alleges, caused the company to lose its once-dominant share of the browser market. On the other hand, scholars view this action as a threat to the conduct of important research. According to Jeffrey Swope, the lawyer for the professors, surrendering the tapes would "stifle or chill future opportunity for research as people would be less willing to participate." Now,

academic researchers are often given access to corporations, as long as they agree not to disclose confidential information or, in some cases, the identity of the business. Such non-disclosure agreements are intended to protect proprietary information; if this information were revealed, access for research purposes could be jeopardized.

Judge Stearns was not convinced that Microsoft's request for the documents met the required tests to force the professors to relinquish their research notes. The three required tests are: 1) that the information sought is not available elsewhere; 2) that the material is relevant to Microsoft's antitrust case; and 3) that the information requested is in the public interest. In a rare ruling from the bench, Stearns stated that Microsoft's arguments were based "on the fundamental premise that a witness in a civil case will lie…As a general proposition, I don't think I can accept that as a judge". Stearns did, however, reserve the right to order the release of parts of the tape should they be required. Microsoft appealed Judge Stearns' ruling.

In December 1998, an appeals panel rule that while "Microsoft's need is admittedly substantial in that relevant information likely exists and Microsoft had a legitimate use for it," the company's need for the tapes did not outweigh the rights of the two professors. The panel noted that Microsoft could return to Judge Stearns' courtroom to seek the materials again if the professors' research turns out to be more vital to Microsoft's defense than it now appears. Tom Pilla, a spokesperson for Microsoft, said that the company is disappointed by the ruling and is reviewing its options.

PRESIDENT SIGNS COPYRIGHT ACT

In October 1998, the President signed the Digital Millenium Copyright Act (DMCA) into Public Law 105-304. The DMCA is designed to bring the United States into compliance with two treaties it signed prepared under the auspices of the World Intellectual Property Organization (WIPO) in 1996. The WIPO treaties grant writers, artist, and other creators of copyrighted materials global protection from piracy in the digital age. Together with the treaties, DMCA seeks to balance the interests of both copyright owners and users.

The House and Senate had originally passed conflicting bills. The bills met with considerable objection from researchers and other scholars. While entertainment and media conglomerates wanted their ownership rights to copyrighted materials secured, researchers wanted to protect their right to use copyrighted materials for educational/research purposes ("fair-use"). The two provisions at the cornerstone of the debate were: 1) the House bill gave database owners the right to safeguard their entire collections of data and prohibit others from extracting information without payment or permission, and 2) the Senate bill made it a crime of circumvention, punishable by fine, to create, sell, or try to override copyright protections.

The final version of DMCA excluded the controversial provision dealing with databases. Additionally, it provides for a two-year study to discover whether technological barriers to copyrighted materials stifle fair-use. The study will be conducted by the Librarian of Congress.

Researchers and educators believe that they gained a major victory, since the DMCA protects non-profit and educational institutions from being sued for copyright infringement because of on-line activities of students, faculty or staff, and access to information found in databases, for the most part, is free of charge. Although database legislation was scrapped in this session of Congress, new legislation is likely to appear again in the 106th session. More information on the DMCA can be found at: http://lcweb.loc.gov/copyright/

NEW GENETIC TESTING POLICY ANNOUNCED IN UK

In November 1998, the British government officially announced that people who have taken genetic tests will get fair treatment from insurers. This announcement comes in response to the Human Genetics Advisory Commission's (HGAC) report, "The Implications of Genetic Testing for Insurance," released in December 1997. The report called for a two-year moratorium on genetic testing by insurance companies, and recommended that the government, the insurance industry, and HGAC work together to establish a new independent evaluation panel on genetic testing, as part of the existing Advisory Committee on Genetic Testing (ACGT).

An independent panel of experts is expected to be in place early next year. The panel will assess whether there is scientific or actuarial evidence that the results of genetic tests provide a sound and accurate basis on which insurance

companies can make decisions about people's insurability. If no clear link is found to exist, test results will not be approved for use by insurers. Science officials, health officials, and the insurance industry have all responded favorably to the announcement of the new panel. Vic Rance, a spokesperson for the Association of British Insurers, stated that "the industry would be very happy to participate in the panel." Science Minister, Lord David Sainsbury, noted that, "Our objective is to put in place a robust system that will meet both the needs of consumers and the insurance industry; and which will also be responsive to the development of genetic science in the future."

Other key points in the governments response to HGAC's report include: 1) ACGT monitoring for any evidence that insurance considerations are deterring people from taking genetic tests; 2) finding ways for the government to strengthen the appeals process for people who believe their genetic information has been used inappropriately; and 3) strong governmental commitment to ensure that unfair discrimination by insurers does not occur. The HGAC report can be found at: http://www.dti.gov.uk/hgac/papers/papers_b.htm

WHISTLEBLOWER CASE DISMISSED

In October 1998, a treason case against Aleksandr Nikitin was dismissed by a judge in St. Petersburg, Russia. Nikitin, an ex-naval officer, was accused by the FSB (Russian successor to KGB) of treason when he reported on Russia's decomissioned nuclear submarines. The disposition of the Russian Northern fleet of nuclear submarines is well-documented, mostly through the efforts of Bellona, the Norwegian ecological foundation. Its 1996 report, drawn entirely from publicly accessible documents, described decommissioned nuclear submarines stored near the Kola peninsula of Russia, the removal of the spent fuel seriously delayed due to political and economic instability in the country. The submarines are rotting in the water, leading potentially to a "Chernobyl in slow motion." During a 1995 raid on Bellona's Russian office, the FSB discovered Nikitin's involvement, claimed that he was endangering Russian security by publicizing state secrets, and arrested him in February 1996. In the following years, seven separate indictments against Nikitin were delivered by the FSB, based for the most part on presumptive violations of secret decrees related to national security and the dissemination of state secrets. The October ruling was thus significant for several reasons. The judge declared the charges were too vague and not based on law. This is the first time in Russian or Soviet history that the FSB/KGB has had a case fail in court. Both sides are appealing the ruling.

The arrest of Nikitin seems to violate not only Russia's own Constitution (Article 42 explicitly prohibits secrecy in any matter that could constitute a hazard to the environment or to the human beings there), but also the United Nations Universal Declaration of Human Rights. Particularly of concern for scientists is the infringement of Article 19 of the UN Covenant on Civil and Political Rights: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive, and impart information and ideas of all kinds, regardless of frontiers…"

As the Nikitin case continues, several issues are in balance. The seriousness of the Russian government about protecting the environment is among these; more pressing, perhaps, is its commitment to free speech. Perhaps most important is what the final outcome will say about rule of law in Russia. Nikitin's lawyer intends to present his case to the international human rights court in Strasbourg, arguing that Russia, with stated goals of becoming an active participant in European culture, economics, and politics, should be held to Western European standards for democracy.

NEW RESEARCH HEATS DEBATE

In November 1998, scientists from academic and non-academic institutions announced progress in human embryonic stem (ES) cell research, reporting that they have established long lived cultures of human cells that have the ability to give rise to any cell in the body. These cells were isolated either from human embryos donated by couples undergoing in vitro fertilization (IVF) as part of treatment for infertility, or from aborted fetuses. The studies were funded by non-federal sources. In the same month, Advanced Cell Technology in Worcester, MA, announced that company scientists had fused adult human cells with enucleated cow eggs, and one of the resulting embryos had divided to yield cells having characteristics similar to those described by the other two groups.

The potential use of such ES cells in improving the quality of human life is enormous, particularly in the generation of cell based therapies for organ transplantation, and for treatment of debilitating diseases such as diabetes and Parkinson's. But the use of these versatile cells can be legally and ethically murky. Currently, there is a Congressional ban on funding research in which an embryo is "destroyed, discarded, or knowingly subjected to the risk of injury or

death." Lawmakers are trying to decide whether the ban applies to the use of those stem cells produced at the University of Wisconsin since they were derived from donated embryos that were to be discarded.

Also, the use of these cells, particularly those derived from human-cow fusion has been opposed on ethical grounds by several groups. Unlike the ES cells developed from embryos, human-animal hybrid eggs may have the potential to develop into a child if transferred into a woman's uterus. Currently, there is insufficient scientific evidence to answer this question. The Senate Subcommittee on Labor, Health, and Human Services held a hearing on the use of ES cells in early December, and the President has requested the National Bioethics Advisory Commission (NBAC) to prepare a comprehensive report on the subject.

UNITED NATIONS BANS CLONING

In December 1998, the 85th General Assembly of the United Nations adopted, without a vote, the Universal Declaration on the Human Genome and Human Rights. This marks the first international action on guidelines for human genome research, including a call for a ban on human cloning.The original draft was adopted by the United Nations Educational, Scientific and Cultural Organization on 11 November 1997; it was then adopted by the United Nations Commission on Human Rights (UNCHR) 19 November 1998.

The Declaration, co-sponsored by 86 countries, emphasizes the need to respect and protect the dignity and human rights of all people without regard to their genetic makeup. It recognizes the importance of freedom of research, and notes that the application of such research is one part of improving health and alleviating suffering. The Declaration emphasizes respect for the differences that occur naturally between individual genomes, research consent and confidentiality, and the control of data gathered from genome research. It sets out to prohibit "practices contrary to human dignity," including reproductive cloning of human beings.

The Declaration is not legally enforceable, but could carry much the same weight as other UN Declarations on Human Rights. Provisions for implementation are included and UNESCO's International Bioethics Committee is encouraged to disseminate and promote the Declaration.

IN THE SOCIETIES

IEEE ETHICS

By Ray Larsen

R.S. Larsen is a past member of the IEEE Ethics Committee. This is an abridged version of an article that originally appeared in The Institute, the newspaper of the IEEE, June 1998.

I want to discuss IEEE Ethics from the perspective of three years of service on the "new" Ethics Committee (EC). The new committee began operations in 1995 with six appointed members, three from the U.S. and three from abroad (currently filled by members from India, Mexico and Germany). The Ethics Committee's main role is advisory to the Board of Directors on all Ethics matters; matters of member discipline or support are vested in the Member Conduct Committee (MCC).

The new EC defined its role in terms of developing a proactive ethics agenda for IEEE. Broadly, it sought to do the following: 1)Promulgate the IEEE Code of Ethics, by having the Code sent to all members with the annual dues, and establishing a webpage; 2)Educate, through a bi-monthly column in The Institute, featuring real examples and various EC member's perspectives; 3)Collaborate, by linking with organizations seeking to promote ethics among engineers and scientists and their employers; and 4)Develop modes of ethics support.

A large effort was directed at Item 4, developing modes of response for members. The Committee saw evidence of need for support of people caught in professional ethical dilemmas. Problem cases were known to members of the EC; moreover, wide promulgation of the Ethics Code by IEEE was felt by the EC as pressure to move in this direction.

Although the EC realized that member support was vested in MCC, the latter had been inactive in promoting itself in this area, so EC felt free to suggest new initiatives to the IEEE Board. Apparently the Board agreed, because it approved nearly unaminously such a proposal, the proposed IEEE Ethics Hotline, in 1996.

The Hotline's announced purpose was to develop a referral service for members. It operated successfully for a year, during which several dozen calls were received, with about a dozen involving clear ethics dilemmas. Some situations concerned the workplace; others concerned IEEE itself, in areas such as publications and standards (plagiarism, peer review, conflict of interest, a student having thesis work published by his academic advisor in an IEEE journal without the student's name, an IEEE Section news organ publishing politically biased materials, a member losing his job through conflicts with a person heading an IEEE standards activity, etc.)

I personally handled about half of these cases. The identity of callers was protected, and a standard disclaimer was made that I was a volunteer, not a trained counselor or legal person. The most serious problems involved situations where a member had been fired over obvious ethical conflicts (e.g., a member disclosing that a major new product contained imbedded software owned by another company; a member reporting to higher management the falsification of semiconductor test data; a member demanding recall of an infant medical device found to have a life-threatening safety problem).

The Hotline taught us the following lessons:

1. *The need for support is real*. A member suffering job loss for ethical behavior is untrained in what to do, is likely to make basic mistakes early that make future legal help ineffective or impossible, and needs to know early how to protect him/herself.

2. *Pro bono (contingency fee) legal help is essentially unavailable to an engineer*. Lawyers will not work on a contingency fee for the relatively small rewards possible through settlement of a case based on unfair job termination

3. *More such problems exist among the members than some might believe*. Only a handful of these were helped through the Hotline because referrals are difficult and IEEE resources are few. Nevertheless, the Hotline boosted the morale of callers.

4. *Fewer such problems exist than IEEE management fears*. Dire predictions of a deluge of "whistleblowers" clogging the Hotline and MCC did not materialize. The average caller was highly principled, sincere, diligent and a very capable engineer, who was finding him/herself in this situation for the first time in his/her career, and was looking for support.

5. *A conflict resolution service would be effective in mediating employee-employer problems before blowup occurred*. Merely having IEEE involved, even at arm's length, would be invaluable in preventing termination over ethics disputes.

In late 1997, the IEEE Board of Directors Executive Committee abruptly terminated the Hotline, citing legal liability concerns. The Ethics Committee and a Special Review Committee appointed by the IEEE President to study the matter both argued that this concern was minimal, based on examples of similar existing operations, but to no avail. In effect, the ExCom reversed the decision of the Board in establishing the Hotline a year earlier. It is unclear whether Excom's problem is only with the Hotline, or a more general fear of becoming involved in the ethics problems of IEEE members. This confusion about the Board's position needs to be clarified both to the EC and to the general membership.

So where do we go from here?

Ethics member support, in my view, is vital to the IEEE and cannot be ignored. But we should not stumble over the Hotline; it is only one facet of a larger, global view of ethics which now squarely challenges IEEE. IEEE has made significant progress in pro mulgating, educating and developing ethics awareness and support within IEEE. Moreover, as a unique transnational engineering society serving a global public, IEEE is positioned to play a defining role in advancing professional ethics globally. This worthy task will demand IEEE's best minds, and should be undertaken with enthusiasm.

I am hopeful that we can meet the challenges in a manner that will bring honor both to IEEE, as a premier global engineering society, and to ourselves, as Professional Engineers who recognize our ethical duty not only to society, but to one another.

AAAS PSEG MEETING

The AAAS Professional Society Ethics Group hosted a meeting in December 1998 to address the effectiveness of the Institutional Review Board (IRB) system in human subjects protection. The meeting featured three speakers:, George Grob, Deputy Inspector General at the Department of Health and Human Services (DHHS), James Bell, of James Bell Associates, and Gary Ellis, Director of the Office for Protection from Research Risks at NIH.

In the course of investigating the improper use of new medical devices prior to final Food and Drug Administration (FDA) approval, the DHHS Office of Inspector General (OIG) discovered various infractions of the human subjects protection system, leading it to conduct a separate study of the system. The OIG sample survey uncovered several indications that the human subjects research review system (which includes IRBs, investigators and research institutions) is under considerable stress. This stress has been attributed to changes in the research environment during the last decade, and includes increases in multi-center trials, private research funding, and the number of human subjects participating in research. The subject culture has also changed notably, as demonstrated by an increase in the demand for access to experimental therapies. The result, according to the report, is that IRBs are reviewing more protocols without a proportional increase in time and resources, thereby reducing their ability to effectively protect human subjects. To alleviate the problem, the OIG made the following recommendations: there should be an increase both in the flexibility of the review process and in IRB accountability, the process of continuing review needs to be strengthened, IRBs should be given the resources they need to accommodate their increased workloads, conflicts of interest between IRB members and their institutions or the research they review must be minimized, and there needs to be an increase in human subjects protection education and awareness. Grob ended his presentation with the observation that there is a culture of care among researchers and IRB members, and that this concern for human subjects will help ensure the success of the system.

Bell, who conducted an IRB study for the NIH Office of Extramural Research, was charged to identify two issues: whether subjects are adequately being protected and whether the system of protection is under undue stress. The first charge was difficult to assess due to the absense of a single mechanism for quantifying the total number of human subjects who have suffered harms from research participation. Bell suggested that a national registry be established to begin tracking such information. His research therefore focused on the IRB review process and his data were presented mainly as percentages of time and effort spent by IRBs of different sizes. The factors that distinguished IRBs from one another were the volume of protocols reviewed and the percent of protocols that qualified for either exemption or expedited review. Bell found a significant variation in the structure of the review process, which reflects the flexibility inherent in the regulations that govern IRB review. This flexibility enables high volume IRBs to appoint more members, and rely more heavily on administrative support to meet increased demands. The percentage of time and effort spent on various activities during actual IRB meetings seem equivalent among the different IRBs. Two thirds of IRB meeting time was spent on initial protocol review, with high volume IRBs that have fewer exempt protocol meeting for longer periods of time. However, the majority of their actual person time spent on initial review occurred before or outside of meeting time, when the administrative staff helps to prepare protocols and coordinate with investigators to facilitate final reviews. Bell concluded that IRBs are not taking advantage of their opportunities to expedite review or exempt specific research protocols, causing them to exert more effort than is necessary; there seems to be an equal distribution of the percentage of biomedical versus social/ behavior research protocols reviewed by IRBs of all sizes, suggesting that the nature of the research itself is not a significant factor in evaluating the quality of the review process; and the total time spent reviewing protocols has not been adversely affected by the general increase in workload because IRBs are successfully utilizing both additional administrative support and the procedural flexibility built into the regulations.

Ellis addressed the global issue of how far human subjects protection regulations actually extend. He focussed on a realm of research that is neither covered by the Federal Common Rule to protect human subjects nor regulated by the FDA. This realm includes research done at IVF clinics, weight loss centers, surveys done through the worldwide web, and some private off-label experimentation. The human subjects who are involved in unregulated, ungoverned research

should be our biggest concern, warned Ellis. He agreed with the National Bioethics Advisory Commission (NBAC) that all human subjects deserve the twin protections of IRB review and informed consent, but was concerned as to how this would be achieved for the most vulnerable subjects. It was noted that NBAC is addressing these issues in its own comprehensive study of the human subjects protection system, due for completion in 1999.

PROPOSED MISCONDUCT POLICY The American Association of University Professors is seeking comment on a proposed policy on misconduct, published in November 1998. The policy was drafted by the Association's Committee B on Professional Ethics to address the responsibilities of faculty members when they suspect colleagues of violating standards of professional conduct. For more information, contact Jonathan Knight at AAUP, 1012 14th St., NW, Washington, DC, 20005; Email jknight@aaup.org. The proposed policy states that:

The American Association of University Professors has long emphasized the obligations assumed by all members of the academic profession, including their responsibility to practice intellectual honesty in teaching and research and not to discriminate against or harass students, colleagues, or other members of the university community. Occasions arise, however, when professors have reason to believe that a faculty colleague has violated standards of professional behavior. When that occurs, professors should take the initiative to inquire about or to protest against apparently unethical conduct.

The initiative can take several forms, from discussion with the professor in question, which may suffice to allay concerns that led to the initial inquiry; to an offer to serve as a mediator; to filing a complaint with appropriate faculty or administrative authorities. Some approaches are tentative and exploratory, while others will be inescapably adversarial.

Inquiry or protest of this sort has its risks. To discuss someone's alleged misconduct with that individual may be neither personally nor professionally easy. It may lead to retaliation and harm to one's career. Moreover, information about the conduct of a colleague may be erroneous or it may be tainted by professional or personal bias. An individual falsely accused may suffer undeserved damage to his or her career or reputation.

But the potential risks do not diminish the obligation of professors to pursue what they believe to be well-founded concerns of professional wrongdoing by other members of the faculty, for the failure to respond can be more damaging. It can result in situations where no one acts at all because each hopes someone else will. And if no one who knows about the alleged misconduct responds, a seeming lack of concern may lead to underestimating or denying its seriousness. Not speaking out may also inadvertently help to sustain conditions in which misconduct is left unchecked or even condoned.

The obligation to speak out is rooted in two considerations. First, in the words of the 1940 Statement of Principles on Academic Freedom and Tenure, institutions of higher education "are conducted for the common good and not to further the interest of either the individual teacher or the institution as a whole." The common good is best served when members of the academic community effectively regulate their own affairs, which they do when they act ethically themselves and also when they seek to ensure such action by others. Second, faculty members are members of a profession, and as such should guard their own standards of professional behavior. To guard is to call attention to abuses of those standards, for in speaking out professors exercise their duty, as members of a self-regulating community, to deal with unethical conduct of a member of the community. In so acting, faculty members promote adherence to norms essential to maintaining the integrity and autonomy of the academic profession.

NEW ETHICS CENTER ESTABLISHED

The American College of Physicians-American Society of Internal Medicine has established the Center for Ethics and Professionalism. The Center will consolidate and implement the College's ethics policy activities and act as a resource to College members and the public.

One of the Center's major projects is the Consensus Panel on end-of-Life Care, a multi-speciality group of experts that is developing a series of papers on end-of-life care issues such as communicating with patients; making decisions and setting goals for palliative care of the dementia patient; pain management; treating depression and delirium; and legal and cultural barriers to good care of the dying. Other projects in 1999 will include ethics case studies, such as ethical dilemmas raised by treating members of one's own family or close friends and conflicts that arise from selling health and non-health related products form a physician's office, statements on ethics, professionalism and managed care, monitoring human rights issues, such as landmines, the effect of political embargoes on the health of nations, and violations of the human rights of individual physicians, and assistance and advice to ACP-ASIM members and the public on ethical issues. "We want to give our current work more visibility, expand the scope of our ethics work and provide a 'think-tank' environment to help put ethics into practice," said Harold C. Sox, President of ACP-ASIM.

RESOURCES

In Print

The ***Princeton Journal of Bioethics*** is a project of the Bioethics Forum of Princeton University aimed at providing an arena for the expression and discussion of issues in bioethics by undergraduate students (first journal is free; a year subscription is $25 for non-students, $5 for students; make checks payable to Bioethics Forum of Princeton University; Dod Hall, Princeton University, Princeton, NJ 08544; E-mail bioethic@ princeton.edu; on-line http://www.princeton.edu/~bioethic.) The Journal is a resource for students and professors of bioethics, as well as a representation of undergraduate work in bioethics. Each issue includes a diverse selection of essays from students, as well as a feature paper from a leading bioethicist.

Research Ethics: Cases and Commentaries, Volume 2, edited by Brian Schrag (Bloomington, IN: Association for Practical and Professional Ethics, $15.00) To order, call (812) 855-6450; Fax (812) 855-3315. As part of a workshop on Graduate Research Ethics Education, a group of graduate and postdoctoral students developed cases exploring major issues in research ethics. The seventeen anonymously-written cases effectively highlight problems facing all working scientists, including concerns about authorship, intellectual property, mentor relations, research on animals and human beings, and compromising research. Some of the cases provide fresh insights into very old problems (e.g., criteria for authorship), while others accentuate more modern concerns (e.g., the responsibilities of mentors to students in tight job markets). All of the examples would be useful for teaching, or as models for students to create their own cases. Included are commentaries written both by the participants and by project faculty. This is an interesting and useful approach and should spark discussions about the nature of the common and differing views of scientists (students and faculty), philosophers, and ethicists.

Early Warning: Cases and Ethical Guidance for Presymptomatic Testing in Genetic Diseases, by David H. Smith, Kimberly A. Quaid, Roger B. Dworkin, Gregory P. Gramelspacher, Judith A. Granbois, and Gail H. Vance (Bloomington, IN: Indiana University Press, 1998 $29.95). To order, call (800) 842-6796; Fax (812) 855-7931. As genetic testing becomes available for a variety of human diseases and accessibility to these tests grows, more genetic counselors will be advising clients on situations involving complex ethical issues. Early Warning is part of a growing literature concerning the difficulties facing the community of human geneticists. This volume is distinguished by its concentration on factual cases with very little generalization drawn from them; the authors suggest that this case-specific approach is most relevant for the clinic. The cases touch on issues including confidentiality, adherence to protocols, and presymptomatic testing of children. They range from situations that are relatively straightforward and resolvable, to the controversial and complex. Despite the emphasis on case analysis, the authors present a set of guidelines as drawn from specific cases, which may be useful as a framework for teaching.

ANNOUNCEMENTS

The conference on **Ethics in Engineering and Computer Science**, sponsored by the Ethics Center for Engineering and Science, will be held on March 21-24, 1999 at Case Western Reserve University in Cleveland, Ohio. The conference will: 1) convene engineers, educators, managers, ethics officers, and engineering and computer ethics scholars to enhance Web resources in ethics of use to engineers and scientists; 2) build on current models of conference collaboration among scholars and teachers to develop new forms of collaboration for building Web resources; and 3) create educational experiences and Web materials that will empower engineering faculty to help their students develop a proficiency in engineering ethics. Contact Caroline Whit-beck, Department of Philosophy, Case Western Reserve University, 10900 Euclid Avenue, Cleveland, Ohio 44106-7119, Email caw9@cwru.edu; WWW http://ethics.cwru.edu

Ethics and Information Technology, a new journal published by Kluwer in 1999, has issued a call for papers. The journal will be dedicated to the study of the ethical dimensions of information and communication technology. For article submission, contact Kluwer Academic Publishers, Journals Editorial Office, Ethics and Information Technology,

P.O. Box 990, 3300 AZ Dordrecht, Netherlands. For subscription information, contact Kluwer Academic Publishers, Order Dept., P.O. Box 322, 3300 AH Dordrecht, Netherlands, Phone [31]78-639 2392; Fax [31]78 654 6474; Email orderdept@wkap.nl; WWW http://www. wkap.nl

The **18th Southern Biomedical Engineering Conference** and the **Second International Conference on Ethical Issues in Biomedical Engineering** has changed its conference date from April 2-4, 1999 to May 20-23, 1999. The conference will be held at Clemson University. Paper are solicited on new developments in theory, concepts, applications, and techniques in all facets of biomedical engineering. Contact Subrata Saha, Ph.D., Director, Bioengineering Alliance of South Carolina, 313 Rhodes Research Center, Clemson University, Clemson, SC 29634-0906; Email: amarand@clemson.edu; WWW http://sbec.abe. msstate. edu

The **University of Texas-Houston Health Science Center** (UT-Houston) will be the location for a "Research Integrity: A Professional, Ethical and Social Obligation," conference on March 11-12, 1999. The conference will focus on shared accountability among members of the scientific community and the general public. Topics include PHS perspectives on research integrity, the roots and origins of scientific integrity, self-deception in research, ethics of authorship and publication, and ethics of randomized clinical trials, public view of biomedical research, setting the biomedical research agenda, and industry sponsorship of research. The fee is $100 for registration before February 15, 1999, and $150 after. Attendance is limited to 200 participants. Contact University of Texas-Houston Health Science Center (713) 500-2028; WWW http://son1.nur.uth.tmc.edu/cnr/ORI.htm

An **EU Advanced Workshop: Biotechnology Ethics and Public Perceptions of Biotechnology** will be held at Oxford, UK, March 19-30, 1999. The course covers biotechnology ethics and practical knowledge for scientists on how to communicate through the media and with the public. Discussions include food biotech issues; patent issues (intellectual property rights, patenting life, plant breeding); ethics and genetic medicine; risk perception and assessment; legal issues and biotechnology. Contact Patricia Osseweijer, Kluyver Laboratory for Biotechnology, Julianlaan 67, 2628 BC Delft, Netherlands, [31] 15 278 5140; Fax [31] 15 782 355; Email p.osseweijer @stm.tudelft.nl

The **Kennedy Institute of Ethics** at Georgetown University and the **College of Health Professions** in cooperation with the College of Veterinary Medicine at the University of Florida will host a conference entitled "The Balanced Evaluation of Animal Research: Fulfilling the Obligations of Science and Society." The conference will be held at the University of Florida on February 6-8, 1999. The program will consider issues of decision-making in a variety of animal-use contexts with a focus on the Institutional Animal Care and Use Committee (IACUC). The conference is intended for biological, biomedical, behavioral, and social scientists, clinicians, students, scholars of the humanities and philosophy, and members of the concerned public. Contact Robbie Eller, Office of the Dean, College of Health Professions, PO Box 100185, University of Florida, Gainesville, Florida 32610-0185; Ph. (352) 392-4215; Fax (352) 392-6529; Email reller@hp.ufl.edu; WWW http://www.hp.ufl.edu.

The **National Science Foundation** offers opportunities for funding in societal dimensions of engineering, science, and technology, science and technology studies and related areas. The Societal Dimensions of Engineering, Science, and Technology Program (SDEST) holds together the former Ethics and Values Studies Program (EVS) and Research on Science and Technology Program. Deadline for proposals is February 1, 1999. Contact Rachelle D. Hollander, SDEST Program Director; Email rholland@nsf.gov; WWW http://www.nsf.gov/sbe/sber/sdest/start.htm. The Science and Technology Studies Program (STS) supports history in history, philosophy, and social studies of science and technology. Deadline for proposals is February 1, 1999. Contact Michael M. Sokal, STS Program Director; Email msokal@nsf.gov; WWW http://www.nsf.gov/sbe/sber/sts/start.htm

The **Office of Research Integrity** is cosponsoring a conference on March 11-12, 1999 with the University of Texas-Houston Health Science Center on "Research Integrity: A Professional, Ethical, and Social Obligation." The conference will focus on shared accountability among members of the scientific community and the general public. The first day will center on the ethical contract among researchers (the professional view) while the second day will deal with the ethical contract with society (the public view). Contact Ria Griffin , Center for Nursing Research, UT-Houston School of Nursing, 1100 Holcombe Blvd., Suite 4.430, Houston, TX. 77030; Ph. (713) 500-2028; Fax (713) 500-2033; Email rgriffin@son1.nur.uth.tmc.edu; WWW http://son1.nur .uthm.tmc.edu/cnr/ORI.htm

AAAS and the **Massachusetts Institute of Technology** are co-sponsoring a colloquium on "Secrecy in Science: Exploring University, Industry, and Government Relationships," March 29, 1999, MIT, Cambridge, MA. The colloquium will focus on restrictions on the sharing and uses of scientific and technical information that challenge traditional norms of openness in science. It will explore current and historical issues of secrecy facing university scientists in their work with industry and government. Registration is free. Contact Amy Crumpton, AAAS, Ph. (202) 326-6792; Fax. (202) 289-4950; Email acrumpto@aaas.org; WWW http://www.aaas.org/spp/secrecy