Emerging ethical issues: Universities and information warfare

Kelly Fisher
Texas A&M University – Kingsville

Jack Shorter
Texas A&M University – Kingsville

ABSTRACT

The nature, the security, and transmission of information have always been of the greatest concern to national defense worldwide. The military complex, along with other governmental agencies, is motivated to place restrictions on any one of these three aspects of information. This has important implications for universities and their faculty. This paper will outline the escalating tensions arising from the sharply distinct cultures of the military and institutions of higher education in post-9/11 America, and their respective and divergent views on the nature and use of information. The paper provides needed insight into the values embedded in the military culture that potentially oppose academic freedom, reinforcing the imperative for universities to proactively manage the ethical choice and publication of their research. This paper's point of view reflects the lead author's prior career in the armed forces. With the recent breaches of security the discussion points in this paper are both topical and timely.

Keywords: Information Warfare, Academic Freedom, Information Operations, Information Assurance, National Security

INTRODUCTION

Researchers are tasked with a number of ethical responsibilities as they gather their data. Arguably, the two fundamental ethical precepts are to seek the truth and serve society (Beck and Kauffman, 1994). In a cautionary report submitted in September 2003 by the American Association of University Professors (Note: AAUP is the leading organization primarily dedicated to protecting the academic freedom of professors.) as a proactive response to the 9/11 attack, their executive summary reinforced the organization's main premise: "that freedom of inquiry and the open exchange of ideas are crucial to the nation's security, and that the nation's security and, ultimately, its well-being are damaged by practices that discourage or impair freedom" (AAUP, 2003). In a recent paper, MacKay and Munro (2012) argue that information warfare will likely become common as both private and public organizations are increasingly sensitive to their informational environment as a source of both opportunity and possible conflict. The AAUP's stated *modus operandus* is at odds with the construct of 'information warfare' as perceived by U.S. military strategists (among others).

The concept of Information Warfare (IW) has been well-documented (for example, Dearth and Williamson, 1996; Denning, 1999; Schwartau, 1996; Waltz, 1998), but may also be referred to as "Information Operations". In times of war and crisis the term "Information Warfare" (IW) is favored by the military; otherwise it is generally referred to as "Information Operations" (IO) which encompasses both peace time and war time operations (Eriksson, 1999). Both terms are used in this paper, depending on the context. The Director of the International Security Studies Core at the Air War College defines IW as "simply the use of information to achieve [American] objectives" (Stein, 1996:1). A slightly different perspective is provided by a United States Air Force report, *Cornerstones of Information Warfare* (1995), which states that Information Warfare "views information as a separate realm, potent weapon, and lucrative target" (p.4). Some military strategists place IW along with nuclear, chemical, and biological weapons as another 'weapon of mass destruction' (Eriksson, 1999). The important differentiation here is between information *in* war and information *as* war. One is a strategy; the other is a weapon. This reflects the seriousness of information as an issue of utmost importance to American national security.

Information as a Weapon

By definition, the fundamental weapon and target in IW is 'information', which is conceived as both a threat and an opportunity and may be manipulated to achieve competitive advantage over others. More than fifteen years ago, Berkowitz (1997) recognized the need to explore the relationship between the military and civilian society in preparing for information warfare, while protecting democratic values—namely, freedom of expression and personal privacy—but taking the measures necessary to defend against an IW threat. Nonetheless, the issues still remain while both technology and information continue to proliferate in a world that is dizzyingly globalized. In this paper it is argued that the military and other governmental agencies with a vested interest in national defense uphold fundamentally different values from academia and that these oppose the open and public dissemination of knowledge where it may negatively impact national security. Political discourse is polarized between those who believe secrets should stay secret and those who believe all information should be made publically available regardless of the fallout produced. Alarmingly, there also appears to be some public consensus that putting the U.S. intelligence community, military and intelligence informant's in harm's way due to the WikiLeaks is being frowned upon by both sides of the political spectrum (democrats and republicans alike). In the light of the 9/11 terrorist attack and the current asymmetric warfare in Iraq and Afghanistan, increased tension between the military and its affiliates and the higher education sector that is focused around the control of information is to be expected and ongoing.

This tension was highlighted when several hundreds of thousands of classified State Department documents were leaked in November 2010 by online whistle-blower WikiLeaks. The dramatic disclosure of classified files has reignited national discussion on the release of protected information in a democratic society. In an article in *The Chronicle Review*, Daniel Drezner (2010) reflected that the released documents had the potential to be a 'game-changer' that would enhance foreign-affairs scholarship. In a much different vein, New York Rep. Peter King, the ranking member of the House Committee on Homeland Security compared the founder of WikiLeaks, Julian Assange, to an "enemy combatant" on national television (Stewart, 2010).

Military educators share a similar viewpoint. At the U.S. Military Academy at West Point, for example, Information Assurance (IA) professors perceive the safeguarding of information systems as a "matter of national security…Our national information infrastructure is not just essential to the U.S. economy; it is a life-critical system" (Ragsdale, D., Welch, D., & Dodge, R , 2003: 64). Within the military ranks, however, the intersection of information and technology extends beyond security concerns: it is perceived as "the most fearsome weapon on the emerging techno-battlefield" (Grier, 1995: 34). Military literature is rife with both real and imagined scenarios involving the hijacking of information off the Internet by terrorist groups for evil purposes. The bio-terrorism in the form of anthrax mailed in letters in October 2001 is still part of the U.S. collective memory and has only added to the weight of conservatives' arguments made by those such as Frankel, Director, Program on Scientific Freedom, Responsibility and Law. Frankel states that research findings should be controlled: "…the primary question for the government, scientific societies, and journals is finding ways to circulate information to those who need to know it, while not 'giving aid to the enemy' (McLellan, 2002: 731).

CONFLICT BETWEEN ACADEMIC FREEDOM AND NATIONAL SECURITY

As the National Research Council (2007: 78) has noted: "historically, the national security and research university communities have "talked past" each other. When discussions do occur, conversations are replete with assumptions and stereotypes." However, the implicit conflict between academic freedom and national security may become quite explicit as conservative elements, especially within the military complex and other public sector organizations, demand tighter control of information. Academic freedom is an issue that impacts upon all university researchers: there are also ethical dilemmas that are of particular importance to researchers and universities who conduct research on or collaborate with organizations in the public sector. This encompasses a broad audience since government sponsored and collaborative research is a major source of research funding for American universities. Over half of higher education's basic R&D research historically comes from federal funds (Organization for Economic Co-Operation and Development, 2003) and in FY2011 Congress proposed $US11.3 billion for Defense Science and Technology (S&T) research alone (AAU, 2011).

Outside academia, however, loyalty to safeguarding the nation is diametrically opposed to the scientist's imperative to openly publish their research. According to the National Security Agency, the nation's security is threatened when national goals and objectives are endangered (*Mission*, 2012). This sweeping concept considers the prevention of another terrorist attack against America and her interests as important as safeguarding critical financial, health, and other quality of life infrastructures (Ruocco, Buchheit & Ragsdale, 2000). Post 9-11 restrictions on information availability, such as new limits on the Freedom of Information Act (*Justice initiative*, 2004), are symptomatic of official concern. We argue that universities should bear in mind that military and government agencies share similar values. Specifically, the National Security Agency/Central Security Service (NSA/CSS), which is currently commanded by an Army general, has established the Information Assurance (IA) department, which operates under the NSA/CSS. The IA department is tasked with the protection of National Security Information and Information Systems, as directed by National Security Directive 42 (“About IA at NSA,” 2012). To further their mission, IA has partnered with academia by developing the National Centers of Academic Excellence in IA Education Program (CAE/IAE) or Research (CAE-R). Schools that meet all nine criteria may be designated as a CAE/IAE or CAE-R. These institutions are then eligible to apply for related scholarships and grants (*National Centers*, 2012). Of specific interest is criterion three, which requires that the university encourage the practice of Information Assurance and not just merely teach the course. An example of a government-based Information Assurance security plan is helpfully provided on the website, but as this paper argues, the aim of the government is to control and restrict the access to information. This is fundamentally at odds with the *raison d’etre* of institutions of higher education.

COMMUNICATION OF RESEARCH AND NATIONAL SECURITY

Research programs may be designated “sensitive” (Greenwood, Li, Prakash, & Deephouse, 2002) according to the U.S. State Department’s Mantis list. (Note: Mantis is a State Department system which was developed to monitor international student visas for study in export controlled technologies, such as nuclear engineering, electronic guidance systems, or munitions. This list also includes nuclear technology, navigation and guidance control, chemical and biotechnology engineering, remote imaging and reconnaissance, information security, lasers and directed energy systems, and robotics.) The problem with this is that many research areas are included that many universities may consider as public domain material. At least one American university, Massachusetts Institute of Technology (MIT) , has already rejected several federal proposals or contracts on research that fell into the ‘sensitive’ category because of the requirement that required access to the project and its results be limited to U.S. citizens (Greenwood et al., 2001).

The crux of the argument used by the military and other conservatives that advocate restricting publication of, or access to, research results is that there is a critical difference in the nature and use of information. The power of the Internet and the ability of terrorist organizations to access a wide range of potentially harmful information have eliminated the traditional barriers of money, people, and physical infrastructure to facilitate acts of war or terror. WikiLeaks has been referred to as the first “stateless news agency”. The analogy has also been made that defending the country from information warfare requires “in effect...the Maginot Line mentality applied to electronic bits” (Ruocco et al., 2000). Academics have a different perspective as MIT’s President Charles M. Vest's asserted in his 2001-02 annual report that it is “the ambiguity and uncertainty of what is inappropriate to publish, or in the use by the government of ill-defined terms like "sensitive but unclassified," that creates danger for the scientific enterprise and invites bad decisions” (Vest, 2002: 1). These same issues are not only still prominent, but as this paper argues, they are increasingly a threat to universities research agendas (Canizares, 2009).

Ethical Tensions and Information Warfare

The process of applying for ethical approval of a proposed research project in a university provides a firm and familiar foundation to examine issues that might be of particular relevance to civilian scientists, if not to military researchers, who are conducting research in collaboration. However, the issues that may arise as a result of collaboration with military organizations (or the acceptance of federal funds tied to military affiliated research) are neither well defined nor well-articulated within the literature regarding research ethics. It is the premise of academic communities that intellectual inquiry is ideally characterized by free expression, free inquiry, and intellectual honesty and the belief that research should be published both widely and promptly (National Research Council, 2007). This paper contends that there is an ideological gap between academia and the military that includes the research arm and military academies of the different armed forces, which should be recognized and addressed within the context of the ethical research approval process. Case in point: an online examination of several leading universities' research ethics policies did not touch upon the topical and important issue of national security in the dissemination of research findings despite their extensive working relationship with the military. This is in stark contrast with the research arms associated with the U.S. armed forces.

For instance, each branch of the military has its own research website, which outlines their organizational research policies. Referring to an online sample of a standard Navy Cooperative Research And Development Agreement, the guidelines state that the "use and dissemination of Information and materials exchanged under this Agreement will be in accordance with all U.S. laws and regulations, including those pertaining to national security and export control" (*Cooperative Research*, 2012). Military policies are in stark contrast to policies esteemed and protected by civilian institutions of higher learning where it is understood that the "free flow of ideas may be a better protection against biological weapons than the secrecy created by classifying academic research" (Powell, 2003, paragraph 1).

Understanding these cultural differences in how information is viewed and ultimately used is necessary to minimizing conflict between universities who hire military researchers or collaborate with a military organization. Further evidence of this ideological gap is shown in a report to the American Association of Universities (AAU) by the Massachusetts Institute of Technology (MIT). In testimony to the U.S. House of Representatives, Canizares (2009) identified increasing attempts by federal agencies to apply "inappropriate restrictions" on basic research as one of the university's current top three concerns. Even in the best-case scenario where agreement can be reached, research projects might be delayed from six months to a year while negotiation for the removal or modification of restrictive language takes place between the stakeholders. Although several universities have proactively established policies that specifically deny the limitation of areas of study or research (Greenwood & Riordan, 2001); others have agreed to censor their research findings (Canizares, 2009).

The potential for information to cause harm, in the context of national security, is an area of ethical and strategic concern for researchers past, present and future. An article in the *New York Times* shortly after the 9/11 attack on America reflected concern by Hellman, professor emeritus at Stanford, about the appropriateness of his and others' decisions in 1975 to defy the National Security Agency's request to classify their ground-breaking cryptography research:

> But now, in the aftermath of the terrorist attacks on New York and the Pentagon, Dr. Hellman and others whose work spawned the commercialization of high-level cryptography are wondering if they did the right thing. They are haunted by the idea that

> law enforcement agencies may have figured out what the terrorists were planning, if only powerful encryption techniques had been kept secret (Kolata, 2001: 1).

In America, memories of broad censorship during the McCarthy era were part of the AAUP's motivation to create the "Special Committee on Academic Freedom and National Security in Times of Crisis" post 9/11. McCarthy was eventually vilified for his anti-Communist crusade conducted from 1950 to 1954, but the shameful memories of his unfounded accusations are still a part of the American collective psyche. Historically, though, before World War II broke out, nuclear scientists instituted a self-imposed ban on publishing matters relating to nuclear fission (Galison, 2004). The result was that Nazi scientists used the ineffective heavy water method (instead of the much more useful graphite) of moderating neutrons to cause fission for the duration of the war. The danger represented by this example, which is still part of the nation's memory, is that there exists a specific case to argue for the restriction of information.

The misuse and misappropriation of information which has been unintentionally or unwittingly disseminated through universities (Greenwood & Riordan, 2002) is of significant interest to military and other governmental organizations, particularly in the areas of science and technology. Information is "fast becoming a strategic national asset" (Fast, 1996: 6). However, this implies a shift in the meaning of "strategic". The specific military meaning has now been extended to include a more general economic and political sense. Information is replacing the traditional economic base of natural resources long used by industrialized nations and this can be linked, in numerous subtle ways to aspects of "national security". Lead time between research efforts and application has become dramatically shorter over the past two decades. Civilian, government, higher education, and military organizations frequently collaborate or share their research efforts (Richardson, Matson, & Peters, 2004). This in turn heightens concern about the military, economic or political advantage that can be maintained from any current and leading edge research. When it comes time to publish, it is quite feasible that a researcher may experience serious conflict between academic integrity versus national security. The ethical code of a researcher demands integrity to the explicit academic norm that knowledge is of the highest good and should have the widest dissemination (National Research Council, 2007). And therein lays the conflict. But the issue will not only be one for the individual researcher to decide. It can be expected that the military will take an increasingly proactive role in the discussion and control of such issues.

This is not an issue confined to the U.S. and its institutions, but is relevant to higher educational entities worldwide as reported by the Open Societies Foundation (2005). Canada, for example, increased limitations to its Access to Information Act in December 2001 when it adopted anti-terrorism legislation. The Irish government also announced in March 2003 that amendments to its own Freedom of Information Act would severely increase restrictions on the release of security and defense information. In Central and Eastern Europe, ten countries have incorporated new state secrets laws which give governments the right to control sensitive information. This list is not inclusive. The United States of America currently has bilateral security standard agreements with fifty-five other countries (*Justice Initiative*, 2004).

INFORMATION, TECHNOLOGY AND GLOBALIZATION

The rapid spread of globalization and the Internet highlights two critical issues regarding the 'nature, security, and transmission' of information. The first is that the United States is "more dependent on electronic information systems than is anyone else in the world…computer and communications systems might prove to be a vulnerable weak link for military forces, there is also a danger that hostile parties--countries, terrorist groups, religious sects, multinational corporations, and so on--could attack civilian information systems directly" (Berkowitz, 1997: 175). Science and technology, coupled with the globalization of communications, have created an environment compared to "the new frontier of combat" (Robbat, 2001). Specifically, the CERT Coordination Center at Carnegie Mellon University, a major reporting center for Internet security violations, recorded 21,756 incidents in 2000, while an astounding 137,529 incidences were reported in 2003 ("CERT statistics," 2012).

The second issue is that the Internet has eliminated traditional barriers to the dissemination of knowledge—a double-edged sword for those concerned with U.S. national security. Over a decade ago, a great deal of concern was generated when research was published showing that insertion of IL-4 genes into mouse pox viruses resulted in near total immunosuppression (Jackson, as cited in Atlas, 2002). Although this study greatly advanced understanding of the immune response, the horror of genetically engineering a deadly strain of smallpox virus made this type of information sensitive in the extreme (Atlas, 2002). A critical issue was that the IL-4 mouse pox study was conducted in Australia; therefore, the U.S. had no jurisdiction over its publication. "It was, however, potentially subject to restraint, raising the question of ethical responsibility within the scientific community" (Atlas 2002: 753). Unlike the Cold War when the U.S. had almost a total monopoly on nuclear weapons development in the 1940s, biotechnology (among other branches of the life sciences) is an international field of study. Given the level of concern in the U.S., it would be naïve to assume that the U.S. government would not seek to exert some control over the publication of material it saw as endangering homeland security.

CONCLUSION

The changing role of information and an increasing recognition of its strategic importance have raised new issues in relation to its ownership and dissemination. The debate on these issues is likely to be conducted in the context of national security and lead, increasingly, to a restriction of the dissemination of research results. Universities will need to be able to define a different context for this argument in order to combat this ideological gap between academic freedom and national security interests, particularly given the billions of federal research dollars at risk. A report issued by the National Research Council (2007) reiterated the need for "maintaining the open exchange of scientific information" and suggested that the federal government establish a standing entity, preferably a Science and Security Commission, that would review policies guiding the exchange of information and the participation of international scientists and students in research.

A proactive and collective recognition by universities that publication of research is both a right and responsibility may encourage individual researchers and their institutions to self-censor their publications. The National Academy of Science, for example, organized a forum for journal editors, scientist-authors, government officials and others, to create a 'Statement on Scientific Publication and Security'. In the preamble, an acknowledgement was made that "fundamental is a view, shared by nearly all, that there is information that, although we cannot now capture it with lists or definitions, presents enough risk of use by terrorists that it should not be published" (NAS, 2003, p.:1149).

Ethical dilemmas necessitate making difficult choices. Although the correlation between innovation and economic growth is widely accepted, consideration of national security issues should be on any research university's horizon. In this paper the authors have set out a perspective that globalization, new information technologies, and the changing nature of knowledge as a national resource, combined with non-state terrorist activities, is an opportunistic breeding ground for the misuse of information that was not conceivable during the Cold War. Also, it would be in the best interests of universities to be proactive in developing a position on these issues now, and not wait for a governmental edict in the future.

REFERENCES

Association of American Universities. (2003). Academic freedom and national security in a time of crisis. Retrieved from http://www.aaup.org/report/academic-freedom-and-national-security-time-crisis

Association of American Universities. (2005). AAU report on the FY2005 Defense/National Security Appropriations. Retrieved from http://www.aau.edu/Search/AdvancedSearch.aspx?id=500

Association of American Universities. (2011) Department of Defense FY 2011 Budget Summary. Retrieved from http://www.aau.edu/publications/reports.aspx?id=6900

Atlas, R. (2002) Bioterrorism: From threat to reality. *Annual Review of Microbiology, 56*: 167-185.

Beck, M.T. & Kauffman, G.B. (1994). Scientific Methodology and Ethics in University Education. *Journal of Chemical Education, 71 (11), 922.*

Berkowitz, B.D. (1997). War in the information age. In J. Arquilla & D. Ronfeldt (eds.), *Athena's camp: Preparing for conflict* (pp. 175- 189). Santa Monica, CA: RAND Corporation.

Canizares, C. (2009, February 25). U.S. House of Representatives testimony, Committee on Science & Technology, Hearing on impact of U.S. export control policies on science and technology activities and competitiveness. Retrieved from http://gop.science.house.gov/Media/hearings/full09/feb25/canizares.pdf

CERT. (2012). *CERT statistics (historical*). Retrieved from http://www.cert.org/stats/#vul-total

Dearth, D.H. & Williamson, C.A. (1996). Information age/Information war. In A.D. Campen, D.H. Dearth, & R.T. Goodden (eds). Cyberwar: Security, strategy, and conflict in the information age, pp. 1-25. Fairfax, VA: AFCEA International Press.

Denning, D.E. (1999). *Information warfare and security*. Reading, MA: Addison Wesley.

Department of the Air Force (1995). *Cornerstones of Information Warfare*. Retrieved from http://www.c4i.org/cornerstones.html

Drezner, D. (2010, December 5th). Why WikiLeaks is bad for scholars. *The Chronicle of Higher Education*. Retrieved from http://chronicle.com/article/Why-WikiLeaks-Is-Bad-for/125628/

Eriksson, E. A. (1999). Information warfare: Hype or reality? *The Nonproliferation Review*, 6(3), 57–64.

Fast, W.R. (1996). Knowledge strategies: Balancing ends, ways, and means in the information age. In R. E. Neilson (ed.), *Sun Tzu and Information Warfare: A collection of winning papers from the Sun Tzu Art of War in Information Warfare Competition* (p. 1-30). U.S. Army War College: Carlisle Barracks, PA.

Galison, P. (2004). Removing knowledge. *Critical Inquiry, 31* (Autumn). Retrieved from http://large.stanford.edu/publications/crime/references/galison/

Greenwood, M. R. C., & Riordan, D. G. (2001). Civic scientist/civic duty. *Science Communication, 231*, 28-40.

Greenwood, R., Li, S.X., Prakash, R., & Deephouse, D.L. (2005). Reputation, diversification, and organizational explanations of performance in professional service firms. *Organization Science*, *16*, 661-673.

Grier, P. (1995). Information warfare. *Air Force Magazine*, 78(3), 34-7.

Open Society Foundations. (2004). National Security and Open Government, Justice Initiative. Retrieved from http://transparentsea.files.wordpress.com/2010/11/access_to_inform.pdf

Open Society Foundations. (2005). National security and open government, justice initiative. Retrieved from http://www.opensocietyfoundations.org/topics/freedom-information

Kolata, G. (2001, September 25). When science inadvertently aids an enemy. *New York Times*. Retrieved January 30, 2013 from http://www.nytimes.com/2001/09/25/science/physical/25TECH.html?pagewanted=1

MacKay, B. & Munro, I. (2012). Information warfare and new organizational landscapes: An inquiry into the ExxonMobil-Greenpeace dispute over climate change. *Organization Studies*, 33 (11), 1507-1536.

McClellan, F. (2002, September 7). Academic freedom or speaking with the enemy? *The Lancet, Vol. 360.* Retrieved from http://www.thelancet.com/pdfs/journals/lancet/PIIS0140673602099373.pdf

National Acadamy of Science. (2003). Statement on Scientific Publication and Security. *Proceedings of the National Academy of Sciences.* Retrieved from http://www.sciencemag.org/site/feature/data/security/statement.pdf.

National Research Council. (2007). Science and security in a Post 9/11 world: A report based on regional discussions between the science and security communities. Washington, DC: The National Academies Press.

National Security Agency. (2012) *About IA at NSA*. Retrieved from http://www.nsa.gov/ia/ia_at_nsa/index.shtml.

National Security Agency. (2012) *Mission*. Retrieved from http://www.nsa.gov/about/mission/index.shtml

National Security Agency. (2012) *National centers of academic excellence*. Retrieved from http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

Organization for Economic Co-operation and Development. (2003). *Steering and funding of research institutions of country report: United States*. Retrieved from http://www.oecd.org/science/scienceandtechnologypolicy/2507966.pdf

Powell, A. (February 27, 2003). *Academic freedom vs. national security discussed: ARCO Forum panel debates benefits, shortcomings of scholarly restrictions.* Retrieved from http://www.news.harvard.edu/gazette/2003/02.27/09-academic.html.

Ragsdale, D., Welch, D., & Dodge, R. (2003, Sept/Oct). Information assurance the West Point way. *Security & Privacy*, *IEEE*, *1*(5), 64- 67.

Richardson, J. J., Matson, W. B. & Peters, R. J. (2004), Innovating science policy: restructuring S&T policy for the twenty-first century. *Review of Policy Research, 21*, 809–828.

Robbat, M.J. (2001). “NOTE: Resolving the legal issues concerning the use of information warfare in the international forum: The reach of the existing legal framework, and the creation of a new paradigm”. Retrieved from http://128.197.26.34/law/central/jd/organizations/journals/scitech/volume6/robbat.pdf

Ruocco, A., Buchheit, N., & Ragsdale, D. (2000). A combined offensive/defensive network model. Proceedings of the 2000 IEEE Workshop on Information Assurance and Security. West Point, NY.

Schwartau, W. (1996). *Information Warfare* (2nd ed). New York: Thunder's Mouth Press.

Stein, G. J. (1996). *Information attack: Information warfare in 2025*. Maxwell Air Force Base, Air War College: Air University Press.

Stewart, R. (2010, December 1). WikiLeaks debate heats up among party leaders. [Web log comment]. Retrieved from http://politicalticker.blogs.cnn.com/2010/12/01/wikileaks-debate-heats-up-among-party-leaders/

United States Naval Research Laboratory. (2011). *Cooperative research and development agreement between the Naval research laboratory (NRL) and xyz corporation (XYZ).* Retrieved from www.nrl.navy.mil.

Vest, C. (2002). Response and responsibility: balancing security and openness in research and education. *Report of the President for the Academic Year 2001-02*. Boston, Massachusetts Institute of Technology.

Waltz, E. (1998) Information Warfare – Principles and Operations. Artech House, Norwood.