P|I|P|S *The Project on International Peace and Security*

The College of William and Mary

POLICY BRIEFS • 2011-2012

The Project on International Peace and Security (PIPS) at the College of William and Mary is a highly selective undergraduate think tank designed to bridge the gap between the academic and policy communities in the area of undergraduate education. The goal of PIPS is to demonstrate that elite students, working with faculty and members of the policy community, can make a meaningful contribution to policy debates. The briefs enclosed are a testament to that mission and the talent and creativity of William and Mary's undergraduates.

Amy Oakes, Director
Dennis A. Smith, Director

The Project on International Peace and Security
The Institute for Theory and Practice of International Relations
Department of Government
The College of William and Mary
P.O. Box 8795
Williamsburg, VA 23187-8795
757.221.5086
pips@wm.edu

TABLE OF CONTENTS

COMBATING RADICALISM IN PAKISTAN: EDUCATIONAL REFORM AND INFORMATION TECHNOLOGY

ALLISON BAER

Pakistan's dysfunctional education system is a major contributor to continuing radicalization that undermines the country's political and economic stability. Previous top-down efforts to reform the education system have met with little success, largely because of Pakistani government corruption or program inefficiency.

This brief proposes that the United States lead the international community in supporting a grassroots initiative to reform Pakistan's education system. Working through a non-profit Pakistani NGO, The Citizens Foundation (TCF), the international community should combine internet resources with traditional education infrastructure to empower the reform efforts of moderates. This approach would involve: (1) further development of TCF curricula and teacher training programs; (2) creation of a free internet-based database in which TCF's curricula and training programs would be available; and (3) construction of urban education centers—similar to former United States Information Agency Libraries and Information Resource Centers—in Pakistan. The aim is to provide moderates with the training and material support necessary to establish better public schools, reform the education system, and reduce radicalization in Pakistan.

The Radicalization of Pakistan

A sizeable minority of Pakistani citizens support radical Islamic movements such as al-Qaeda, the Afghan Taliban, and Tehrik-i-Taliban. Moreover, backing for radical groups also has increased in the military.[1]

- In 2011, there were almost 2,000 terrorist attacks in Pakistan, in addition to 301 clashes between security forces and militants.[2]

- In May 2011, 12% of Pakistanis said they view al-Qaeda favorably. Over 15% of Pakistanis support the Afghan and Tehrik-i-Taliban and 27% support the anti-India Islamic group Lashkar-e-Taiba.[3]

- General Ashfaq Kayani, Pakistan's Chief of Army Staff, did not condemn the recent murder of the Governor of Punjab and prominent social liberal, Salman Taseer. Amhed Rashid, a well-known Pakistani journalist, stated that the General declined to comment because "too many soldiers in the ranks…sympathize with the killer…[and] any public statement…could endanger the army's unity."[4]

Radicalization and Pakistan's Public Education System

Pakistan's struggling public education system is a major contributor to radicalization.[5] Public schools use radical curricula, receive inadequate funding, and do not prepare students for the workforce. Professor Tariq Rahman of Quaid-i-Azam University, Islamabad, stated that students "succeed in spite of the [education] system not because of it."[6] As a result, undereducated or unemployed Pakistanis turn to extremist organizations that promise societal and economic change. [7]

- *Radical Content of Curricula*: Rubina Saigol, a Pakistani academic studying public school textbooks, found that "a great deal of the ideology that we think madrassas are producing is in fact being produced in state schools."[8] Public school curricula teach that Islam and Pakistan are in danger and that the Pakistani people are at war with the West.[9] Thus, 30% of undergraduates surveyed in 2010 ranked the United States as the largest threat to Pakistan.[10]

- *Underfunded Education System*: Ahmed Rashid reported that in Pakistan "social services, especially education, remain abysmal, because every year the government's spending on…education is cut."[11] Because the Pakistani government allocates less than 3% of GDP to education, Pakistan was ranked 142 out of 163 countries for percentage of GDP spent on education in 2009.[12] Consequently, 20,000 schools lack sufficient facilities; others are over-crowded or are non-existent "ghost schools."[13] 66% of parents identified "non-availability" of schools as the reason why their child was not enrolled.[14] The student-to-teacher ratio in primary schools is 40:1 and teachers earn as little as $50 per month.[15]

- *Lack of Job Training*: A 2007 UNESCO report asserted that Pakistan needs to "re-conceptualize the role of technical and vocational education and to link it to primary and secondary education."[16] Professor Khadim Hussain of Pakistan's Bahria University stated that students "don't understand what evidence is" and that many are taught that using "logic means that you are definitely an agent of India."[17] Having few vocational or analytical skills leaves students susceptible to radical propaganda and unprepared for the job market.

Radicalization and Pakistan's Madrassas

Six percent of Pakistani students attend private Islamic schools, called madrassas, largely because they are closer, lower cost, or have better resources than public schools. Other students attend madrassas because their parents prefer they receive a religious education.[18] However, madrassas use archaic curricula that do not provide vocational skills and some madrassas directly recruit students for terrorist operations.

- *Impractical and Outdated Curricula*: Christine Fair, an Assistant Professor at Georgetown University, notes that the Pakistani government would like "madrassas students to be more employable."[19] Half of madrassas' standardized curricula are religious studies. The remaining content is the "rational sciences," including math, medicine, astronomy, history, philosophy, polemics, and prosody. The most recent texts in the rational sciences curricula date to the 14th century.[20]

- *Militant Recruitment*: Tariq Rahman asserts that "the *madrassa* are the most intolerant of all other student groups in Pakistan."[21] Approximately 23% of Pakistani militants have attended a madrassa, and 13% were recruited at their madrassa.[22]

Pakistan's public education system lacks funding and appropriate curricula. Madrassas fail to prepare students for the global economy or themselves recruit students for militant organizations. Therefore, education reform is necessary to counter the spread of radicalism in Pakistan.

Past Attempts to Reform Pakistan's Education System

The Pakistani government, the international community, and the United States recognize the connection between the country's failing education system and radicalization. In response, they have implemented a variety of reform initiatives.

Domestic Reform Initiatives

Pakistan's national and provincial governments have attempted multiple reforms, such as the Education Sector Reforms and the establishment of the Punjab Education Foundation.

- The *Education Sector Reforms* (ESR) were begun by the Ministry of Education in 2001 as part of the international Education for All initiative. ESR targeted school availability, institutional reforms, vocational and technical training, education quality, and the integration of private schools into the public system.[23]

- The *Punjab Education Foundation*, funded by Punjab's provincial government, provides free private schooling to students. Current enrollment is estimated at 600,000.[24]

Assessment: Political divisions in Pakistan greatly hinder national education reforms, such as ESR. For instance, conservatives have vehemently opposed the ESR goals of integrating madrassas and revising the national curricula.[25] Successful provincial reforms, such as the Punjab Education Foundation, are not standardized throughout Pakistan, limiting their effectiveness.[26]

International Education Initiatives

The international community gives both bilateral and multilateral education aid to Pakistan. Two prominent multilateral efforts are the World Bank's Education for All initiative and the United Nations' World Food Program.

- *Education for All* is an initiative that seeks to improve access to high quality education, lessen gender disparities, and improve adult literacy.[27]

- The *United Nations World Food Program* provides food to students and rations to families in order to improve women's education, enrollment, and performance levels.[28]

Assessment: Most international aid projects underperform because Pakistan's education bureaucracy is corrupt and underfunded or the program allocates resources inefficiently.[29] The Education for All Global Monitoring Report noted that Pakistan has made "slower progress" in increasing enrollment than other participants.[30] The World Food Program has also experienced difficulties: providing food to some schools has caused students already enrolled elsewhere to switch schools, but has not increased total student enrollment in the country.[31]

U.S. Education Initiatives

The United States provides $200 million annually to Pakistan in education aid.[32] USAID supervises five initiatives: Links to Learning, Children's Television Project, Fulbright Scholarship Program, Teachers Education Program, and Higher Education Commission Support.

- *Links to Learning* improves achievement in English, science, math, and computer literacy by increasing teacher training and education infrastructure.[33]

- *Children's Television Project* uses television and other media to develop language, problem-solving, and critical thinking skills.[34]

- *Fulbright Scholarship Program* increases the number of Pakistanis qualified to be leaders in education, society, politics, and business by providing scholarships to elite Pakistani students pursuing graduate degrees in the United States.[35]

- *Teachers Education Program* works with Pakistani universities, training programs, and education departments to better educate and train Pakistani teachers.[36]

- *Higher Education Commission Support* is developing financial aid programs with 11 universities and the Higher Education Commission in Pakistan. The program helps institutions establish permanent financial aid programs, scholarships, and relations with international institutions. It also funds students affected by the 2010 floods.[37]

Assessment: U.S. education aid is ineffective because of Pakistani government corruption, a lack of U.S. oversight, and Pakistani resistance to secular education.[38] Of the $1.5 billion given to Pakistan under the Enhanced Partnership with Pakistan Act (EPPA) in 2010, only $180 million was properly allocated.[39] In addition, a 2008 report from the Brookings Institution found that Pakistanis view U.S. attempts to "secularize" curricula as invasive.[40]

Demand for Education Revitalization by Pakistani Citizens

Pakistanis are frustrated with extremist violence and believe it to be increasingly detrimental to the state.

- 63% of Pakistanis fear Islamic extremism because it produces violence, has a negative impact on the economy, increases division in the country, and results in loss of civil liberties.[41]

- Following Osama bin Laden's death, 60% of Punjabis fear that extremists may seize control of Pakistan and 56% consider extremists a "serious threat" to Pakistan.[42]

Pakistani citizens are combating radicalization through multiple grassroots initiatives, several of which work to increase the availability and quality of education.

- Dar ul Uloom Ashraf al-Madrassas Okara, a school in Okara, Pakistan, is re-educating radical youths and developing non-radical curricula. Specifically, the school promotes a peaceful understanding of *jihad* and emphasizes the concept of peace in the Koran.[43]

- The 2011 UNESCO Education for All report states that "NGOs [in Pakistan] have established 'satellite schools' in consultation with community leaders in areas where government schools have been destroyed by the Taliban."[44]

- In Abbottabad, citizens want the government to establish a women's college on land that was previously part of bin Laden's compound.[45]

Using Information Technology and Improved Infrastructure to Revitalize Education

Pakistani citizens increasingly recognize the importance of education for reducing extremism. In light of the failure of previous reform efforts, citizens are developing their own grassroots initiatives to improve education. The Arab Spring has demonstrated that grassroots movements in non-Western countries benefit from internet access, as it allows for widespread information sharing and communication. Therefore, the United States should lead a multilateral effort to: (1) support a moderate grassroots organization in Pakistan, The Citizens Foundation; (2) provide digital education resources and; (3) improve internet and education infrastructure in Pakistan.

Benefits of Expanding The Citizens Foundation

TCF's presence and success in multiple regions of Pakistan makes it well-positioned to lead and coordinate grassroots reform efforts.

- *Record of Success in Pakistan*: TCF runs 730 schools in over 80 towns and cities. Its current enrollment is over 100,000 students, nearly half of whom are female.[46]

- *Community Involvement*: Upon entering a community, TCF establishes positive relationships with reluctant community members, making it popular among Pakistanis.[47]

- *International Branches*: TCF has fundraising branches in the United States, the United Kingdom, Canada, the United Arab Emirates, and Bahrain.[48]

- *Fundraising Capabilities*: TCF funds all infrastructure and operating costs through tuition and private donations from individuals or corporations.[49]

- *Moderate Curricula*: TCF's curricula combine national education goals with international curricula to achieve the "personal and moral development" of students.[50]

- *Successful Training of Employees*: TCF's training program provides pre-service and in-service training for teachers. Its training team regularly updates the training manual.[51]

Because of its popularity within Pakistan and existing international infrastructure, TCF has the resources and expertise necessary to lead a grassroots education revitalization project. Thus, the United States should encourage countries with international branches of TCF to assist with and fund the establishment of an education database and education centers.

Education Database

The education database will supply TCF curricula and training resources to teachers, students, and citizens, regardless of school affiliation or location.[52] Database resources will include:

- *School Curricula*: The database will offer online access to TCF textbooks, activities, labs, assignments, and exams.

- *Continuing Education Courses and Curricula*: The database will provide online courses for Pakistani adults interested in improving their education. Importantly, it will also provide curricula that will assist Pakistani educators interested in teaching adult education courses.

- *Teacher Training Resources*: The database will include TCF recommended resources on teaching strategies and classroom management. There will also be information about higher education programs, further teacher training opportunities, foreign exchange programs, and scholarships.

Education Centers

Education centers will be located throughout Pakistan, primarily in urban areas to ensure access for the largest number of citizens. Each center will be equipped with the following:

- *Computer Lab*: Each computer lab will be open to the public and will have free internet access. Computers will require log-in for use, allowing TCF employees to detect any usage by radicals. All computers will have desktop links to the education database, as well as reputable news sites. Computer labs will have a printer and photocopier to facilitate the distribution of free educational materials.

- *Library*: The libraries will have copies of textbooks available on the education database, subscriptions to newspapers, journals, and magazines, and copies of both Pakistani and foreign books. Libraries will be a space for academic study and research and will loan materials to registered citizens.

- *Lecture Hall or Classroom*: Each center will provide a lecture hall or classroom for use by the public schools, or for teacher training sessions, adult-education courses, public meetings, and lectures—either in person or via teleconference—by academics and specialists.

Advantages of TCF Education Database and Education Centers

Advantage #1: Reduces Radicalization and Empowers Moderate Education Reform Efforts

- *Competition for Madrassas*: Education centers will help lessen the appeal of madrassas by giving public school teachers access to additional resources.

- *Moderate Islamic Curricula*: TCF curricula will be an alternative to unpopular secular curricula and curricula currently taught in public schools and madrassas. The database curricula will allow educators to both please parents and eliminate radical messages from the classroom.[53]

- *Teacher Training*: Teachers will be able to continue their own education by using training resources available online and in the education centers, improving the quality of educators throughout Pakistan.

- *Continuing Adult Education*: Education centers will hold adult education courses and the database will provide online classes for adults. Increasing overall education in the country will lead to greater economic opportunities and lessen the appeal of radicalism.

- *Research*: Education centers will provide access to the internet, which will allow Pakistanis to research topics of interest, making them better informed and therefore less susceptible radical propaganda.

Advantage #2: Reduces Radicalization through Increased Employment

- *TCF Employees*: TCF will hire local Pakistanis, especially women, to run and maintain the education centers and database. In addition, TCF will hire Pakistanis to work as security guards for education centers.

- *Career Advancement*: Pakistanis will be able to attend education center classes and use center computers for vocational training, improving their credentials and ability to find a job.

Advantage #3: Universal Access to Database and Improved Internet Infrastructure

- *Database Access*: The education database will provide educational resources to teachers and students who have internet access, but are unable to visit an education center.

- *Internet Infrastructure*: Education centers will increase internet access in urban areas by providing such access free of charge.

Advantage #4: Pakistani Citizen Involvement

- *Project Evaluation*: Pakistanis working in an education center will report on the success of the center and the usefulness of the database. They will monitor local enthusiasm for the project and provide suggestions for improvement.

- *Resource Suggestions*: Pakistanis will be able to suggest new materials that should be added to the database or stocked in education center library collections, increasing the likelihood that the resources will be useful to the population.

Advantage #5: Minimal Involvement of the Pakistani Government

- *Implementation*: TCF is legally registered in Pakistan as a private company and is able to receive international donations.[54] Therefore, the Pakistani government will be less able or likely to block implementation or insist on government oversight.

- *Funding*: Foreign governments, international donors, and citizens will fund the aid initiative. It will not rely on Pakistani government funding and will thus avoid diverting funds from national education programs or losing funds due to government corruption.

Possible Objections

Objection #1: Education Center Internet Access Will Further Spread Radical Propaganda

- Radical groups could use improved internet access to disseminate more propaganda, recruit followers, and coordinate attacks in Pakistan.[55]

- The internet allows radicals to recruit and build relationships with individuals outside of Pakistan.[56]

Response: Education centers will be able to monitor computer use and prevent center computers from being used to circulate radical propaganda.

Objection #2: Militants Will Target Education Centers

- In October 2009, two suicide attacks were carried out at the International Islamic University, killing at least six people. The day after the attacks, schools throughout the country were closed due to safety concerns.[57]

Response: TCF hires guards and gatekeepers for their schools to guarantee their safety.[58] Some TCF schools are also located inside army compounds to ensure security.[59] The education centers will make use of the expertise and successful system of TCF to guarantee security. The database will provide educational resources to areas that TCF judges too dangerous for a center.

Objection #3: Pakistanis' Distrust of the United States

- Pakistanis may view an education reform initiative led by the United States as imperialist.[60]

- Pakistanis currently resent U.S. aid because it has traditionally focused on the military, while the population lacks essential government services.[61]

Response: First, basing the education database content on TCF curricula and teacher training programs will reduce accusations of imperialism. Second, since the program will support an existing internal movement for better education, Pakistanis may be more receptive.[62] The international community will be clear that is providing the support that moderates have requested.[63] Finally, the program will be more popular than other aid initiatives because it will focus on the long-term development of Pakistan, as opposed to short-term U.S. military or strategic goals.

Objection #4: Opposition from the Pakistani Government or Military

A 2011 Congressional Research Service Report highlights reactions by Pakistani officials and military officers to the EPPA:

- The report describes officials as "highly critical of the EPPA, seeing in its language an intent to interfere with and dictate to Pakistan on sensitive foreign policy and national security issues, perhaps even with malicious goals."[64]

- In addition, the Pakistani military expressed "serious concern regarding clauses [of the law] impacting on national security."[65]

Response: Working with TCF will diminish Pakistani government involvement and interference because TCF is already registered as a business and legally operating in Pakistan. In addition, TCF's mechanism to receive funds from international branches is already in place and requires no further involvement of the Pakistani government.[66] Finally, implementation of the project does not require concessions from the civilian government or military.

Objection #5: Reluctance of the U.S. Government

- Current U.S.-Pakistan relations have been increasingly strained since the Abbottabad raid in May 2011. More investment in Pakistan may not be seen as worthwhile at present.[67]

- The United States has already committed to giving Pakistan $7.5 billion in non-military aid under the EPPA; it may be hesitant to use further funds during an economic recession.[68]

- The United States dislikes funding multilateral organizations or leading multilateral efforts.[69]

- The U.S. Congress may be hesitant to fund a program that integrates religion and education.

Response: First, expanding TCF will benefit U.S.-Pakistan relations, as Pakistanis may become more cooperative once they have received aid that successfully benefits the populace. And, since TCF is able to build and operate a school for a year for less than $90,000, this proposal will be a comparatively low-cost method for improving relations with Pakistan.[70] Second, the United States has previously funded religious education in other countries.[71] In addition, a 2003 report by the USAID Bureau for Policy and Program Coordination recommended that, to improve education in Islamic countries, USAID should support moderate Islamic education initiatives, in addition to secular efforts.[72]

Conclusion

Radicals are a threat to the stability of the international community, the security of Pakistan's nuclear arsenal, and U.S. forces in the region. Reforming the education system will decrease Pakistani support of radicals, but government corruption, a lack of coordination, program inefficiency, and misguided objectives have impeded past and current reform efforts.

International funding of TCF to create an education database and establish education centers will empower moderate Pakistanis, improve the quality of public education, and reduce the appeal of madrassas. The initiative will provide the moderate majority of Pakistanis with the resources they need to reform the education system from the bottom up. Public schools will benefit from physical infrastructure, modern curricula, and better trained teachers. As the quality of public schools increases, enrollment in madrassas will decrease. Thus, a better educated Pakistani

populace, less prone to radicalization, and with better prospects for employment, will emerge, improving domestic stability and regional stability, and U.S.-Pakistan relations.

[1] Fareed Zakaria, "The Radicalization of Pakistan's military," *The Washington Post*, June 22, 2011, http://www.washingtonpost.com/opinions/the-radicalization-of-pakistans-military/2011/06/22/AGbCBSgH_story.html.

[2] Pak Institute for Peace Studies, *Pakistan Security Report 2011* (Islamabad: Pak Institute for Peace Studies, January 2012), 5, http://san-pips.com/.

[3] Pew Research Center, *Support for Campaign against Extremists Wanes: U.S. Image in Pakistan Falls No Further Following bin Laden Killing* (Washington, DC: Pew Global Attitudes Project, June 21, 2011), http://www.pewglobal.org/2011/06/21/u-s-image-in-pakistan-falls-no-further-following-bin-laden-killing/.

[4] Ahmed Rashid, "An Army without a Country," *New York Review Blog*, The New York Times Review of Books, March 4, 2011, http://www.nybooks.com/blogs/nyrblog/2011/mar/04/army-without-country/.

[5] UNESCO Education for All, *EFA Global Monitoring Report 2011: The Hidden Crisis: Armed Conflict and Education* (Paris: United Nations Educational, Scientific and Cultural Organization, 2011), 262, 265, http://unesdoc.unesco.org/images/0019/001907/190743e.pdf.

A 2011 UNESCO report ranked Pakistan's education system 119 out of 127 countries. The rankings are based on primary enrollment, adult literacy, gender equality, and quality of education through grade 5.

[6] Tariq Rahman, "The Educational Caste System: A Survey of Schooling and Polarization in Pakistan," *tariqrahman.net*, http://www.tariqrahman.net/educa/DENIZENS%20OF%20ALIEN%20WORLDS%20Amended.htm.

[7] Muhammad Azam, "Radicalization in Pakistan: Sociocultural Realities," *Conflict and Peace Studies* 2, no. 1 (January-March 2009): 10, http://san-pips.com/download.php?f=06.pdf.

C. Christine Fair, "The Educated Militants of Pakistan: Implications for Pakistan's Domestic Security," *Contemporary South Asia* 16, no. 1 (March 2008): 100-101, http://home.comcast.net/~christine_fair/pubs/Fair_CSA_2008.pdf.

Given that 58% of militants completed a secondary level of education, a large percentage, one-quarter, were unemployed or underemployed in the year before they were recruited.

[8] *Pakistan: The Lost Generation*, Documentary, directed by David Montero, (PBS Frontline World, February 12, 2010), http://www.pbs.org/frontlineworld/stories/pakistan901/video_index.html.

[9] PBS, "Pakistan: The Lost Generation: Story Synopsis," *Frontline World: Stories from a Small Planet*, http://www.pbs.org/frontlineworld/stories/pakistan901/video_index.html.

[10] Pak Institute for Peace Studies, *Radicalization: Perceptions of Educated Youth in Pakistan* (Islamabad, Pak Institute for Peace Studies, September 20, 2010), 11, http://san-pips.com/download.php?f=45.pdf.

[11] Ahmed Rashid, *Pakistan on the Brink: The Future of America, Pakistan, and Afghanistan* (New York: Viking, 2012), 32.

[12] UNESCO, *Education (All Levels) Profile-Pakistan*, UIS Statistics in Brief (Paris: United Nations Educational, Social and Cultural Organization Institute for Statistics, 2011), 3, http://stats.uis.unesco.org/unesco/TableViewer/document.aspx?ReportId=289&IF_Language=eng&BR_Country=5860&BR_Region=40535.

U.S. Central Intelligence Agency, *The World Factbook: Country Comparison, Education Expenditures* (Washington, DC: CIA), https://www.cia.gov/library/publications/the-world-factbook/rankorder/2206rank.html.

[13] Montero, *Pakistan: The Lost Generation*.

PBS, "Pakistan: The Lost Generation: Story Synopsis."

Sixty percent of Pakistani schools have no electricity; forty percent have no available drinking water.

[14] UNESCO, *Education (All Levels) Profile-Pakistan.*

Masooda Bano, *Education for All by 2015: Will We Make It? Pakistan: Country Case Study*, Education for All Global Monitoring Report 2008 (Paris: United Nations Educational, Social and Cultural Organization, 2007), 23, http://unesdoc.unesco.org/images/0015/001555/155503e.pdf.

[15] Griff Witte, "Poor Schooling Slows Anti-Terrorism Effort in Pakistan," *The Washington Post*, January 17, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/01/16/AR2010011602660.html.

The wages of some teachers in Pakistan are lower than that of domestic servants.

[16] Bano, *Education for All by 2015*, 32.
UNESCO, *World Data on Education: Pakistan*, 7th ed. (Paris: United Nations Educational, Social and Cultural Organization International Bureau of Education, 2010-2011), 21, http://unesdoc.unesco.org/images/0021/002113/211310e.pdf.
In addition, a 2011 UNESCO assessment reported that Pakistani students "were found weak in the competencies/skills of writing and comprehension in languages, problem-solving and sums involving use of currency and conversion in the subject of mathematics, and life skills knowledge in the subjects of science/general knowledge."
[17] Witte, "Poor Schooling Slows."
[18] Mumtaz Ahmad, "Madrassa Education in Pakistan and Bangladesh," in *Religious Radicalism and Security in South Asia*, eds. Satu P. Limaye, Mohan Malik, and Robert G. Wirsing (Honolulu, Hawaii: Asia-Pacific Center for Security Studies, 2004), 108, http://www.apcss.org/Publications/Edited%20Volumes/ReligiousRadicalism/PagesfromReligiousRadicalismandSecurityinSouthAsiach5.pdf.
Declan Walsh, "Pakistan Schools Campaign Hopes to Avert 'Education Emergency,' British-backed Initiative Aims to Help Overhaul a System that Has Left Seven Million Children without Primary Education," *The Guardian*, March 8, 2011, http://www.guardian.co.uk/world/2011/mar/08/pakistan-faces-education-emergency.
UNESCO Education for All, *EFA Global Monitoring Report 2011*, 195.
[19] C. Christine Fair, *Islamic Education in Pakistan* (Washington, DC: United States Institute of Peace, March 2006), 7, http://home.comcast.net/~christine_fair/pubs/trip_report.pdf.
[20] Ibid., 3.
[21] Rahman, "The Educational Caste System."
[22]Fair, "The Educated Militants of Pakistan," 100.
Taimoor Shah and Alissa J. Rubin, "2 Boys with Suicide Vests Are Arrested in Afghanistan," *The New York Times*, February, 12, 2012, 1, www.nytimes.com/2012/02/13/world/asia/2-boys-with-suicide-vests-are-arrested-in-afghanistan.html.
Pakistani madrassas are also known to recruit children for suicide missions in Afghanistan. In February 2012, a 12-year-old boy who attended a madrassa in Quetta reported that his teachers said, "You won't be hurt; just go and carry out a suicide attack."
[23] Government of Pakistan Ministry of Education, *Education Sector Reforms: Action Plan 2001-02 - 2005-2006* (March 2004), 9, 13-14, http://www.moe.gov.pk/esr/Chap2.pdf.
[24] Sir Michael Barber, "Education Reform in Pakistan: This Time It's Going to Be Different," *Pakistan Education Task Force* (June 2010), 5, http://pakistaneducationtaskforce.com/erp.pdf.
[25] K. Alan Kronstadt, *Education Reform in Pakistan* (Washington, DC: Congressional Research Service, December 23, 2004), 6, http://www.au.af.mil/au/awc/awcgate/crs/rs22009.pdf.
[26] Barber, "Education Reform in Pakistan," 5.
[27] The World Bank, "Education for All (EFA): What is Education for All (EFA)?" *Education: Human Development Network*, http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTEDUCATION/0,,contentMDK:20374062~menuPK:540090~pagePK:148956~piPK:216618~theSitePK:282386,00.html.
[28] Touseef Ahmed and others, "Food for Education Improves Girls' Education: The Pakistan Girls' Education Programme," *School & Health* (March 9, 2007), 3-4, http://www.schoolsandhealth.org/sites/ffe/Key%20Information/Food%20for%20Education%20Improves%20Girls%E2%80%99%20Education__Tshe%20Pakistan%20Girls%E2%80%99%20Education%20Programme.pdf.
United Nations, "Pakistan: WFP Activities," *World Food Programme*, http://www.wfp.org/countries/Pakistan/Operations.
[29]Senate Committee on Foreign Relations, *Educating the Pakistani Masses: The World Needs to Help, Combating Terrorism through Education: The Near East and South Asian Experience: Shahid Javed Burki*, 111th Cong., 1st session, April 19, 2009, 9, http://www.foreign.senate.gov/imo/media/doc/BurkiTestimony050419.pdf.
Shahid Javed Burki's testimony described Pakistan's education bureaucracy as "corrupt, inefficient and dysfunctional" and cited it as a cause of failed international aid efforts.
[30] UNESCO Education for All, *EFA Global Monitoring Report 2011*, 42.

[31] World Food Programme, *Case Study: Pakistan-Girls' Education on the Frontline*, Learning from Experience: Case Studies (Rome, Italy: United Nations World Food Programme), 3-4, http://documents.wfp.org/stellent/groups/public/documents/newsroom/wfp207493.pdf.
[32] Witte, "Poor Schooling Slows."
[33] USAID, "Links to Learning: Education Support to Pakistan (ED-LINKS)," *USAID/Pakistan*, http://www.usaid.gov/pk/sectors/education/edlinks.html.
[34] USAID, "Education: Children's Television Project," *USAID/Pakistan*, http://www.usaid.gov/pk/db/sectors/education/project_33.html.
[35] USAID, "Education Overall Fact Sheet," *USAID/Pakistan: Fact Sheets*, http://www.usaid.gov/pk/sectors/education/docs/ed_factsheet.pdf.
USAID, "USAID-Fulbright Scholarship Program," *USAID/Pakistan*, http://www.usaid.gov/pk/sectors/education/ufs.html.
[36] USAID, "News Release: U.S. Supports Teacher Education Reforms in Pakistan," *USAID/Pakistan*, July 6, 2011, http://www.usaid.gov/pk/newsroom/news/education/110706.html.
USAID, "Higher Education Commission – Financial Aid Development (HEC-FAD) Program," *USAID/Pakistan*, http://www.usaid.gov/pk/sectors/education/hecfad.html.
[37] USAID, "Education: Higher Education Commission Support – University Development," *USAID/Pakistan*, http://www.usaid.gov/pk/db/sectors/education/project_2.html.
[38] Susan B. Epstein and K. Alan Kronstadt, *Pakistan: U.S. Foreign Assistance* (Washington, DC: Congressional Research Service, June 7, 2011), 27, http://fpc.state.gov/documents/organization/166839.pdf.
A 2011 CRS report on U.S. foreign assistance to Pakistan stated that U.S. programs suffer from corruption and need more U.S. oversight.
[39] U.S. Government Accountability Office, *Department of State's Report to Congress and U.S. Oversight of Civilian Assistance to Pakistan Can be Further Enhanced*, (Washington, DC: United States Government Accountability Office, February 17, 2011), 8, http://www.gao.gov/assets/100/97299.pdf.
[40] Moeed Yusuf, *Prospects of Youth Radicalization in Pakistan: Implications for U.S. Policy*, The Brookings Project on U.S. Relations with the Islamic World, Analysis Paper 14 (Washington, DC: The Brookings Institute, October 2008), 20, http://www.brookings.edu/~/media/Files/rc/papers/2008/10_pakistan_yusuf/10_pakistan_yusuf.pdf.
[41] Pew Research Center, *Support for Campaign.*
[42] Ibid.
[43] Mehreen Farooq and Waleed Ziad, "The Battle for Pakistan's Soul," *Foreign Policy: The AfPak Channel* (September 1, 2011), http://afpak.foreignpolicy.com/posts/2011/09/01/the_battle_for_pakistans_soul.
[44] UNESCO Education for All, *EFA Global Monitoring Report 2011*, 224.
[45] Muhammad Sadaqat, "Residents Want Girls College Built on Ruins of OBL Compound," *The Express Tribune*, February 28, 2012, http://tribune.com.pk/story/342810/residents-want-girls-college-built-on-ruins-of-obl-compound/.
Citizens of Abbottabad argue that "our daughters, the future mothers, will disseminate the message of peace and non-violence across the area, if the authorities allow construction of a girls college."
[46] The Citizens Foundation, "Milestones," http://www.thecitizensfoundation.org/Milestones.aspx.
[47] Ashan Saleem, "Against the Tide: Role of The Citizens Foundation in Pakistani Education," in *Education Reform in Pakistan: Building for the Future*, ed. Robert M. Hathaway, (Washington, DC: Woodrow Wilson International Center for Scholars Asia Program, 2005), 79, http://www.wilsoncenter.org/sites/default/files/FinalPDF.pdf.
Marie Lall, *Creating Agents of Positive Change-The Citizens Foundation in Pakistan* (Karachi, PAK: The Citizens Foundation, Autumn 2008), 36, http://www.thecitizensfoundation.org/ePanel/Resources/DownloadFiles/Publications/Category/8/36/Marie%20Lall%20Report.pdf.
A 2008 report by Dr. Marie Lall of the University of London found that "parents across the board wanted to see more TCF schools," indicating the popularity of the Foundation in Pakistan.
[48] The Citizens Foundation, "TCF Supporters," http://www.thecitizensfoundation.org/Supporters.aspx.
[49] Saleem, "Against the Tide," 71-72.
TCF schools cost roughly $70,000 to build and $13,000 in annual operations' costs.
[50] The Citizens Foundation, "Curricula," http://www.thecitizensfoundation.org/Curricula.aspx.
[51] The Citizens Foundation, "Training," http://www.thecitizensfoundation.org/Training_Evaluation.aspx.

[52] The education database will be structured similarly to the Multimedia Educational Resource for Learning and Online Teaching (MERLOT) website.
MERLOT, *Multimedia Educational Resource for Learning and Online Teaching*, http://www.merlot.org/merlot/index.htm.
[53] Fair, *Islamic Education in Pakistan*, 8.
Pakistani parents are concerned that their children both receive an education and learn to be "good Muslims."
[54] The Citizens Foundation, "TCF Story."
The Citizens Foundation, "TCF Supporters," http://www.thecitizensfoundation.org/Supporters.aspx.
[55] Raffaello Pantucci, "The Jihad Will be YouTubed," *Foreign Policy: The AfPak Channel* (December 15, 2011), http://afpak.foreignpolicy.com/posts/2011/12/15/the_jihad_will_be_youtubed.
The Washington Post, "U.S. Military, Taliban Use Twitter to Wage War," *The Washington Post with Foreign Policy*, December 2011, http://www.washingtonpost.com/world/asia_pacific/us-military-taliban-use-twitter-to-wage-war/2011/12/16/gIQAKnJ32O_story_1.html.
Merlyna Lim, "Islamic Radicalism and Anti-Americanism in Indonesia: The Role of the Internet," *Policy Studies* 18 (2005): 43, 45, 48, http://scholarspace.manoa.hawaii.edu/bitstream/handle/10125/3520/PS018.pdf?sequence=1.
[56] Susan Collins and Joseph Lieberman, *Violent Islamist Extremism, The Internet, and the Homegrown Terrorist Threat: Majority & Minority Staff Report,* Senate Committee on Homeland Security and International Affairs, 110th Cong., 2nd sess., (May 8, 2008), 3, 11, http://www.dtic.mil/dtic/tr/fulltext/u2/a482218.pdf.
Max Entman, *Audio: Interview with Rick "Ozzie" Nelson on Homegrown Extremism*, Center for Strategic and International Studies (September 29, 2010), http://csis.org/multimedia/audio-interview-rick-ozzie-nelson-homegrown-extremism.
[57] Salman Masood, "Schools in Pakistan Closed in Wake of Attack," *The New York Times*, October 21, 2009, http://www.nytimes.com/2009/10/22/world/asia/22pstan.html.
[58] Lall, *Creating Agents of Positive Change*, 19.
[59] Ibid., 29.
[60] Bryan Gibel, "Pakistan: The Lost Generation: US Aid to Pakistan: The Kerry-Luger Bill," *Frontline World: Stories from a Small Planet*, PBS, http://www.pbs.org/frontlineworld/stories/pakistan901/aid.html.
[61] Ibid.
[62] Farooq and Ziad, "The Battle for Pakistan's Soul."
[63] Ibid.
[64] Epstein and Kronstadt, *Pakistan: U.S. Foreign Assistance*, 8.
[65] Ibid., 9.
[66] The Citizens Foundation, "Our Schools," http://www.thecitizensfoundation.org/schoolList.aspx.
[67] K. Alan Kronstadt, *Pakistan-U.S. Relations: A Summary* (Washington, DC: Congressional Research Service, October 21, 2011), 2, 5, 7-9, 30-31, http://www.fas.org/sgp/crs/row/R41832.pdf.
After the raid on Abbottad, many members of the U.S. Congress began to question why the United States should continue to send aid to a country that supports militant Islamic groups and where Osama bin Laden was able to live comfortably for several years. The United States also feels that Pakistan is not cooperative enough, given the amount of U.S. aid it receives.
[68] *Enhanced Partnership of Pakistan Act 2009*, S. 1707, 111th Cong., 1st sess., *Congressional Record* 155, no. 148 (October 15, 2009), http://www.govtrack.us/congress/bill.xpd?bill=s111-1707&tab=summary.
[69] Marian L. Lawson and Curt Tarnoff, *Foreign Aid: An Introduction to U.S. Programs and Policy* (Washington, DC: Congressional Research Service, April 9, 2009), 9, http://fpc.state.gov/documents/organization/124970.pdf.
[70] Saleem, "Against the Tide," 71.
The Citizens Foundation, "Our Schools."
TCF schools have class and art rooms, administration rooms, a playground, library, and computer and science labs. Thus, TCF is able to construct and maintain these facilities for a year for less than $90,000.
[71] David B. Ottaway and Joe Stephens, "From U.S., the ABC's of Jihad: Violent Soviet-Era Textbooks Complicate Afghan Education Efforts," *The Washington Post*, March 23, 2002, http://www.washingtonpost.com/ac2/wp-dyn/A5339-2002Mar22?language=printer.
During the Cold War, the United States supplied Afghanistan with textbooks containing militant Islamic teachings.
[72] USAID Bureau for Policy and Program Coordination, *Strengthening Education in the*

Muslim World: Summary of the Desk Study, Issue Paper No. 2 (Washington, DC: United States Agency for International Development, 2003), http://www.devtechsys.com/assets/Uploads/docs/publications/strengthening-education-in-the-muslim-world-summary.pdf.

THE ACTIVE DENIAL SYSTEM: OBSTACLES AND PROMISE

BENJAMIN BUCH AND KATHERINE MITCHELL

The Active Denial System (ADS) is a non-lethal weapons technology that uses millimeter-wave directed energy to arrest and deter potential adversaries. Developed by the Air Force Research Laboratory and the Department of Defense's Non-Lethal Weapons Program, ADS provides U.S. forces with a highly effective means of responding to potential threats while also preserving human life.

Despite its promise, ADS has confronted non-technological challenges in its deployment, most recently in Afghanistan. This brief analyzes the political, psychological, and sociological barriers to the use of non-lethal directed energy weapons. Specifically, it surveys the psychological and sociological biases against radiation-based and non-lethal technology and how these prejudices were overcome in the past. It also examines potential human rights concerns and political complications that might arise from the deployment of ADS in population protection operations. Given these obstacles, the report proposes a series of recommendations for the use of ADS moving forward.

The Changing Nature of Warfare

The two decades following the conclusion of the Cold War have presented a new strategic and operational landscape for American military planners. The overwhelming conventional superiority of the United States has encouraged adversaries to adopt unconventional asymmetric strategies and tactics.

Rise of Asymmetric Conflict

Given U.S. conventional military supremacy, American forces have increasingly encountered adversaries who seek to exploit asymmetries in vulnerability, logistics, and organization through the novel use of strategy, tactics, and technology. This asymmetric form of warfare avoids traditional force-on-force confrontations in which U.S. forces dominate. Instead, adversaries seek and use relatively low-cost means to increase U.S. military and civilian casualties and hinder operations. In addition, these adversaries have shown a growing tendency to harness information networks to affect the perceptions of decision-makers and populations in the United States, the host nation, and the international community.[1]

Implications for Population Centric Warfare

Population centric warfare involves those conflicts in which the outcome depends on garnering and maintaining the support of local and domestic populations, normally associated with peacekeeping and counterinsurgency (COIN) operations.[2] Due to the rise of asymmetric strategies and tactics, U.S. forces can expect adversaries to increasingly take advantage of aversion to military and civilian casualties in order to weaken popular support for U.S. operations. Part of such an effort will be adopting strategies that bait U.S. forces into overusing their conventional superiority in an attempt to cause greater civilian casualties and collateral damage. This aversion reinforces the importance to operational planners of adopting alternative metrics of mission success in population centric warfare, such as:

- Number of civilian casualties;
- Collateral damage to civilian infrastructure; and
- Domestic and international public opinion.[3]

Moreover, population-centric warfare reinforces the need for U.S. forces to have a wide range of non-lethal force options in order to limit civilian casualties and collateral damage when engaged in peacekeeping and COIN operations.[4]

The Promise of ADS

The use of conventional lethal and non-lethal weaponry by U.S. forces may cause civilian casualties and collateral damage, alienating local populations.[5] However, ADS is a revolutionary non-lethal weapon that could mitigate many of the problems U.S. troops face in population protection missions. ADS uses millimeter wave technology to heat moisture just below the skin's surface, creating an intense sensation of heat. This sensation prompts an immediate and reflexive flight response in the target.

ADS is a unique technology for four reasons:

1. *ADS is a single weapon that can provide a spectrum of deterrence options.*

   Unlike lethal weapons and a variety of non-lethal weapons—such as the TASER, rubber bullets, pepper spray, and tear gas—ADS can operate along a wide spectrum of deterrence, as the frequency of its millimeter wave is adjustable. The device can also be used for a single warning or the repeated deterrence of human targets.

2. *ADS does not physically damage its targets*.

The intense sensation of heat caused by ADS allows troops or law enforcement to protect themselves and their assets without having to resort to lethal or even harmful force. When operated in the 94-95 GHz frequency range, ADS's millimeter wave has no long term adverse health effects. ADS's ability to leave its targets uninjured, painless, and fully functional post-use is a revolutionary feature in the realm of non-lethal weapons technology. A 2008 Human Effects Advisory Panel study showed that ADS repels its targets at a lower temperature than would cause first- or second-degree burns, and causes no pain, injury, or incapacitation as soon as targets step out of the millimeter wave beam. During the only incident in which ADS has been shown to produce injury, it was found that, because of a technical malfunction, ADS had been operated outside of its standard power and duration settings.[6]

3. *ADS acts on single human targets, minimizing collateral damage.*

   Unlike other non-lethal weapons systems, like the Long Range Acoustic Device (LRAD) or chemical crowd control systems, ADS's energy beam can precisely target individuals.[7] This feature allows U.S. forces to selectively deter instigators or potential perpetrators of violence, while minimizing harm to innocent bystanders.

4. *ADS acts at a range and efficacy unprecedented in the realm of non-lethal technology.*

   ADS exceeds the range of traditional non-lethal weapons allowing for effective use far beyond the effective range of small arms.[8] In addition, traditional forms of protection against non-lethal weapons, like thick clothing, do not counter ADS's millimeter wave.[9]

<u>ADS: Technical Specifications</u>

In response to its early promise, ADS was designated an Advanced Concept Technology Demonstration between 2002 and 2007.[10] Two ADS models were produced from this process:

- *System 1* is mounted on a modified High Mobility Multi-Purpose Wheeled Vehicle (HMMWV); and

- *System 2* is a self-contained, box-shaped model transportable via tactical vehicles larger than the HMMWV.

Both systems use a millimeter wave generator that operates in the 94-95 GHz range. In 2008, System 2 underwent a Capabilities and Liabilities review and was deemed ready for deployment.[11]

Initial Deployment and Public Response

In 2010, ADS was introduced into two theaters—U.S. COIN operations in Afghanistan and the Los Angeles County prison system—and then withdrawn.[12]

ADS attracted wide coverage in the media during and after its initial deployment.[13] While most early coverage was neutral and focused on the technical development of ADS, later coverage emphasized both the positive and negative aspects of the technology.

- Positive media coverage centered on the ability of ADS to limit civilian deaths, its utility in dispersing mass demonstrations, and its technologically novel aspects, such as its range, economic value, and ability to limit collateral damage.[14]

- Meanwhile, negative media coverage focused on the "science fiction" nature of the technology (i.e., its ability to cause pain from a distance), the potential for a backlash among target populations in theaters of use, and possible unanticipated adverse health effects.[15]

Political Barriers to the Deployment of ADS

Two characteristics of ADS's millimeter wave technology pose political problems for its successful deployment:

1. *ADS has the potential to cause severe pain without leaving a visible mark or physically harming its target.*

2. *ADS acts silently and invisibly*.

These two characteristics produce the following political obstacles to the use of ADS:

Human Rights Concerns

Unethical regimes or personnel could easily deny abuses of ADS, as the device leaves no physical evidence of its use. In addition, because ADS is a new and radiation-based technology, there is fear that exposure could lead to long-term health effects. While few human rights organizations have explicitly commented on ADS, many have expressed deep concerns regarding the use of non-lethal weapons: An analysis of these concerns can help shed light on likely future objections to ADS deployment and use.[16]

- *Amnesty International*: Amnesty International has been the most outspoken critic of non-lethal weapons, particularly of conducted energy devices (CEDs).[17] It has recommended the recall of all non-lethal weapons on the grounds that their abuse

is easy to conceal, and that they are potentially deadly if used on targets with some medical conditions.[18]

- *Human Rights Watch*: Human Rights Watch does not oppose the use of non-lethal technology on principle; in fact, it has supported their use as an alternative to lethal force in places like New York City, Kazakhstan, Tibet, Yemen, and Uganda.[19] However, in a 2007 interview, Marc Garlasco, a former senior military expert for the organization, argued that, although ADS is preferred to lethal force, it has the potential to be used excessively due to its non-lethal nature. Law enforcement literature confirms Garlasco's fear that the availability of non-lethal force can prompt an "increase in the total incidence of force."[20] Garlasco also expressed concern about ADS's long-term health effects.[21]

- *United Nations*: In 2004, the UN's Special Rapporteur on Torture Theo van Boven released a report on the development and sale of technology specifically designed to inflict pain.[22] In Article 30 of the report, Van Boven concluded that non-lethal weapons could be used for "torture and ill-treatment" and recommended extensive testing, "stringent training [for their use], and restrictions on their transfer."[23]

All of these organizations speculate that states and non-state actors alike could easily abuse non-lethal weapons with impunity, given that they leave no physical trace. In a 1997 report, Amnesty International alleged that twelve states, including the United States, had abused CEDs.[24] Additionally, Human Rights Watch and United Nations officials worry that there has been insufficient testing of the long-term medical effects of non-lethal weapon use, especially testing that examines how non-lethal weapon exposure will interact with pre-existing medical conditions.

Psychological and Sociological Biases

There is currently a low level of awareness of ADS among the general public. However, ADS is similar to other radiation-based technologies with which the public is familiar and researchers have documented an entrenched psychological bias against these technologies. This bias is likely to pose a significant obstacle to the use of ADS at home and abroad. For example:

- In a 2000 study, Lennart Sjoberg reported that radiation was one of the four most frightening phenomena according to approximately 700 participants who were surveyed about a variety of terrifying situations. Additionally, when asked about a Chernobyl-like nuclear disaster, participants indicated that they were more afraid of the mere presence of radiation than the actual catastrophic nature of the accident. The participants also said that they felt radiation technology was "tampering with nature".[25]

- A number of psychological studies have shown that radiation is one of the four main "modern health worries" that have resulted from the emergence of new technologies.[26] Individuals for whom radiation is a primary worry also reported experiencing increased physical sensitivity to the effects of radiation-based technologies.[27]

- Victims of nuclear accidents, such as those in Chernobyl in 1986 or Fukushima in 2011, suffer from more persistent psychological trauma than victims of natural disasters where the physical damage incurred was of a comparable scale.[28]

There are two characteristics of radiation technology that most worry the public and could cause it to view ADS as a particularly frightening weapon:

1. *Radiation has the potential to cause permanent damage.*

   Unlike conventional weapons, radiation is known not only to cause immediate contamination but also long-term, irreversible biological damage.[29] The potential for permanent injury underlies the fear of and hostility towards radiation technologies. For example, there was a substantial public backlash to the use of depleted uranium ammunition in the Gulf War by U.S. forces in the early 1990s.[30] Despite medical testing that indicates the technology is safe, ADS's use of radiation could also spark fears that it is carcinogenic.[31]

2. *Radiation invisibly penetrates the human body.*

   Traditional weapons, like bullets, cause successive levels of pain as they visibly penetrate a target's body. But like other radiation-based technologies, the effect of ADS is invisible. Its millimeter wave imperceptibly and inaudibly causes a sensation of burning under the surface of the skin and cornea while leaving the skin's outer surface intact.

   Radiation's invisible penetration of the human body is problematic for the acceptance of ADS on two levels.

   First, the ability of radiation to leave no trace while causing internal damage gives radiation technologies the stigma of "tampering with nature."[32] As such, they are viewed as more frightening than new technologies that use more conventional delivery mechanisms.[33] Because ADS could be perceived as invisibly tampering with human biology, it is more likely to be met with public resistance than other forms of non-lethal weaponry.

   Second, in cultures where folklore plays a significant role in group identities, ADS may be perceived as a magical or supernatural instrument of evil. Therefore,

ADS has the potential to be used as a tool to turn the population against U.S. military operations.

Insurgent and counterinsurgent leaders alike have manipulated local beliefs in superstition for strategic gain in asymmetric conflicts, such as those in the Philippines, the Congo, and India.[34] For example, the Filipino government scared away Han rebels from their strongholds in 1953 by convincing them that vampires resided there.

Consequently, ADS could be a powerful propaganda tool for insurgents in missions like Afghan COIN operations, where tribal populations hold superstitions against invisible "jinns" who cause misfortune or illness.[35] Because ADS acts with no visible cause-effect mechanism, U.S. forces will have difficulty proving to target populations that ADS is not the root cause of later misfortunes among them.[36] Furthermore, insurgent leaders may convince local populations that, even when they do not feel the burning sensation that accompanies ADS, they are continuously exposed to radiation because of the presence of ADS.

Acceptance of new technology occurs not only through spreading awareness of its benefits, but also through a long-term process of socialization.[37] Conducting a few successful and effective test missions will be crucial in helping domestic and foreign populations understand ADS's safety and usefulness.

Further, ADS deployment must be accompanied by aggressive efforts to gain the support of tribal or traditional authorities for use of the weapon. Any information campaign addressing the fears of ADS within a population must take into account local norms, religions, and superstitions.

Legal Challenges

The increase of non-lethal weapon use in combat has raised concerns regarding their compliance with the two principles of *in jus bello*, or the legal concept of "justice in war".[38]

- *Discrimination*: *In jus bello* dictates that force must not be used against noncombatants. While the application of this concept within the framework of lethal force is straightforward, its application to the use of non-lethal weapons is contested, as non-lethal weapons are often used with the express knowledge that they may target civilians.[39]

- *Proportionality*: *In jus bello* dictates that "enemy combatants should not be subjected to unnecessary suffering and superfluous injury."[40]

The potential legal obstacle to the use of non-lethal weapons is that they "reduce lethality by making force itself less lethal while also *increasing* the likelihood of civilian exposure

to that force."[41] For ADS in particular, discrimination is a bigger concern than proportionality. The utility of ADS to the U.S. Armed Forces lies in its ability to determine the intent of approaching individuals; therefore, ADS's mandate is, in part, to be used against non-combatants. As Human Rights Watch's Marc Garlasco discussed, the use of ADS is ethically and legally problematic because it is likely to be employed more frequently against non-combatants than lethal weapons.

While ADS does not violate any explicit international statues on weapon use in military operations, the 1997 Additional Protocol to the Geneva Conventions provides concrete legal guidelines that should shape future ADS deployments. Article 35.2 of the Additional Protocol reads: "it is prohibited to employ weapons, projectiles, and methods of warfare of a nature to cause superfluous injury or unnecessary suffering." Therefore, when ADS is used, the group responsible for deployment must demonstrate that it does not cause superfluous injury or unnecessary suffering.[42]

Recommendations for Fielding and Improving ADS

This brief presents a series of recommendations for combating the potential obstacles to the use of ADS. It is crucial that these political barriers are overcome if ADS is to be employed in conflicts where population support is a key metric for success.

Human Rights Concerns

Human rights organizations are primarily concerned with three possibilities:

- *ADS will be abused without leaving physical evidence on its victims.*
- *Because ADS is non-lethal, operators will feel more comfortable using it either indiscriminately or more often.*
- *ADS may cause long-term health effects and be lethal to targets with prior medical conditions.*

To combat these concerns, this brief recommends the following:

- *Recommendation #1*: Limit ADS ownership to U.S. forces or allies with strong human rights records.

  While the United States can enforce standard operating procedures for ADS among U.S. operators, it cannot control how ADS is used by other states. In light of the sensitive nature of ADS, we recommend that ADS or civilian-made equivalents (e.g., Raytheon's "Silent Guardian") should not be sold to foreign actors through Foreign Military Sales (FMS) or Direct Commercial Sale (DCS), except to close allies with strong human rights records.

At present, ADS has not been labeled by the DOD as a "program of record," and, therefore, it does not qualify for transfer under the FMS program.[43] However, this does not preclude the sale of civilian-produced equivalents, such as the "Silent Guardian," through the process of DCS.[44] Additionally, the DOD should take steps to ensure that ADS does not fall into the hands of irresponsible or unstable foreign actors through theft of the device.

Preventing unwanted foreign acquisition of ADS is particularly important as the technology has not yet been used in a large-scale deployment by U.S. forces. If abused by foreign governments, the technology will lose much of its strategic utility for U.S. forces. In addition to eliminating an existing technological superiority, foreign use will undermine U.S. efforts to encourage a positive public perception of the device. More specifically, the misuse of ADS technology by foreign governments likely will result in the weapon being labeled as a tool of oppression.

- *Recommendation #2*: Equip ADS units with video recording systems and establish a credible chain of command for the recordings of ADS use.

  Every ADS unit should be equipped with a tamper-proof video recording mechanism that tracks the user, date, time, duration, and beam intensity of each instance when the millimeter wave is fired and sends this data to a central database. Similar recording mechanisms are found in the TASER's AXON device, which exports video recordings of police TASER use to an external database via a camera attached to the officer's head. This allows officers to show the precise situations they faced when using the TASER. A digital fingerprint on each file ensures that the video recordings in the central database cannot be tampered with.[45] Recordings of ADS uses should regularly be made available to the international media, human rights organizations, and senior commanders to demonstrate the appropriate use of the device.[46]

  This modification will serve two important purposes:

  First, keeping permanent records of ADS uses will protect U.S. troops from wrongful prosecution should hostile target populations make false allegations of abuse. Mitigating the potential for such accusations will not only assuage fears that U.S. troops may have about using this technology, but will also protect the reputation of the U.S. Armed Forces internationally and among populations where ADS is deployed.

  Second, installing a permanent data recording and transmission capability will help the United States identify any ADS abuse by its forces. This capability will allow the United States to punish those operators who violate the established standard operating procedures.

- *Recommendation #3*: Outline clear operational and tactical doctrines.

  ADS deployment and operational training should include a "Use of Force Continuum," such as the one employed by many U.S. police departments, and should look to protocols for the use of CEDs, like the TASER, as models.[47] For example, by developing a new doctrine that linked specific suspect behaviors with appropriate responses, the Orlando Police Department doctrine substantially improved the public image of CEDs.[48] In the case of ADS, it will be important to tailor these tactical doctrines to the specific operational conditions in each theater where ADS is used.[49]

- *Recommendation #4*: When possible, publicize the punishment of any troops who abuse ADS.

  It will be important to demonstrate to both the U.S public and the international community that there will be tough oversight of ADS use. Police departments in the United States and abroad have sought to reassure a skeptical public by widely publicizing incidents in which officers were punished for CED-related infractions.[50] This practice would be particularly important when deploying a system in a delicate operational environment, such as COIN. Therefore, when military guidelines permit, any punishments following incidents of abuse should be publicized to demonstrate that the U.S. Armed Forces are committed to maintaining a positive relationship with populations among whom ADS is deployed.

- *Recommendation #5*: Fund independent medical research on health conditions that could make the use of ADS dangerous.

  The U.S. government should fund further independent research on medical conditions that may amplify the severity of ADS's effects. Additional research will increase public confidence in the findings of the 2008 Human Effects Advisory Panel study of ADS. CEDs faced similar concerns and, in response, studies were conducted to determine the effect of CED use on targets that had different levels of intoxication or preexisting heart conditions.[51]

<u>Psychological, Sociological, and Legal Concerns</u>

The use of millimeter wave radiation by ADS raises four psychological, sociological, and legal obstacles to public acceptance of the device:

- *Even harmless irradiation is widely associated with permanent damage.*

- *Radiation is perceived as "tampering with nature."*

- *Due to its invisible, inaudible operating mechanism, the use of ADS may be exploited by adversaries in theaters of use where local superstitions are rampant.*

- *ADS violates the discrimination principle of jus bello. In trying to use ADS to determine intent, operators will likely target innocents as well as belligerents.*

To combat these concerns, this brief recommends the following:

- *Recommendation #6*: Associate ADS with commonplace radiation technologies in public relations campaigns.

  Associating ADS with a harmless device, such as the airport body scanner that uses similar millimeter wave radiation, will encourage a positive (or at least neutral) view of the technology. Not only will this association quell fears that ADS could cause permanently harmful health effects, but it will diminish ADS's current negative association with microwave oven technology and the corresponding fear of being 'cooked' when exposed to its beam.

- *Recommendation #7*: Rename ADS.

  Operators should choose a name for ADS that is free of negative language like "denial." Renaming the device will help limit the association of ADS with negative terms like "pain ray" or "microwave" that are prevalent in media coverage, which reinforce stereotypes that all radiation technologies tamper with nature.

  Additionally, ADS should be given a name that emphasizes its use as a tool of non-lethal engagement and cooperation with target populations. In the case of LRAD, the military focused on the loudspeaker aspect of the device to reinforce the perception that it is mainly a defensive system. LRAD was labeled an "acoustic hailing device," which emphasized that its purpose is to warn and communicate with civilians.[52] "Active denial" indicates that operators of the system are opposed to their targets, even if those targets are innocent or are approaching U.S.-manned posts to seek council or to express legitimate grievances. This notion is counterproductive to the goals of population-centric U.S. missions.

  Any new name should emphasize the defensive aspects of the system or its role in determining target intent. For example: Area Defense System (ADS), Non-lethal Intent Determination System (NLIDS), or Millimeter Wave Deterrence System (MWDS).[53]

- *Recommendation #8*: Include optional warning mechanisms with ADS.

  Introducing warning signals with ADS is an important step towards mitigating public fear of the device due to the invisibility of its beam. A warning signal would be a particularly useful addition to the device in theaters where the local population has superstitions against invisible, malevolent entities.

  Most audio and visual warning systems have a shorter range than ADS and, therefore, would be ineffective. However, the laser dazzler, a non-lethal weapons technology that uses laser technology to cause temporary vision impairment and disorientation in subjects could be an effective warning system. Unlike traditional warning mechanisms, it has a range similar to that of ADS. Pairing ADS with a laser dazzler would allow operators to provide targets with early warning and allow for a greater spectrum of deterrence. For example, a laser dazzler could signal to an individual that he or she is being targeted by ADS. If the dazzler fails to deter a target, then ADS could be used to inflict increasing levels of pain, starting with a mild sensation of heat and progressing to an intense burning sensation, to alter the target's behavior.

  Another option would be a warning system where potential targets could opt to receive cell phone messages announcing when the device is present or in use. This warning system would require cooperation with authorities with access to the local phone systems. But the primary advantage of a warning system would be that it allows direct interaction with a sizeable portion of the target population, further mitigating the negative political and psychological effects of ADS use.[54]

  A warning system, combined with clear tactical doctrines and recording mechanisms, also demonstrates the desire to minimize its use on civilians. These steps will go a long way to mitigate concerns of ADS violating the discrimination principle of *jus bello* legal theory.

- *Recommendation #9*: Hold domestic public demonstrations coinciding with deployment.

  When ADS is introduced in a theater, it should be frequently and publicly demonstrated to preempt misperceptions or rumors. A common tactic to promote CED acceptance has been public demonstrations on local police officers.[55]

  The "media days" held to demonstrate ADS between 2007 and 2012 are examples of such outreach campaigns. Any future deployment should include further outreach efforts, not only in the United States, but also among target populations. Ideally, demonstrations will include local elites, as respected leaders will play a critical role in encouraging positive dialogue about the technology.

- *Recommendation #10*: Publicize the challenges necessitating the deployment of ADS.

  Another important step to overcoming political barriers to ADS deployment is to convince the American public of the need for ADS to protect our soldiers in the field. Before deployment, the need for ADS should be explained to the U.S. population. This outreach effort should include short films chronicling life for soldiers manning checkpoints or tasked with base defense in Afghanistan.

  These outreach efforts should be distributed through traditional media and online media distribution sources, including YouTube. Current ADS demonstration videos have already reached a wide audience, displaying the potential of online media for shaping public perception of ADS.

Conclusion

ADS is a promising non-lethal technology for the U.S. Armed Forces, performing an important role in an era where U.S. military engagements are defined by population protection. To be deployed successfully, however, ADS must overcome political, sociological, and psychological barriers among the U.S. public and target populations. Public acceptance of ADS is crucial both to achieve domestic support for its deployment, as well as to facilitate the very purpose of ADS, which is to foster a positive relationship between the U.S. Armed Forces and the populations among which they operate. In this brief, we have identified the primary barriers to the successful use of ADS and have suggested steps that the U.S. military can take to address these concerns. Should these barriers be overcome, ADS has the potential to become the vanguard technology of an emerging class of weapons that fill a crucial gap in the current capabilities of the U.S. Armed Forces.

[1] For more on the rise of asymmetric warfare, see: Col. T.X. Hammes, *The Sling and the Stone: On War in the 21st Century*, (St. Paul, MN: Zenith, 2004). Ivan Arreguin-Toft, "How the Weak Win Wars: A Theory of Asymmetric Conflict," *International Security* 26, no. 1 (2001). Tim Benbow, "Irresistible Force or Immoveable Object? The "Revolution in Military Affairs" and Asymmetric Warfare," *Defense and Security Analysis* 25, no. 1 (2009). John Galvin, "Uncomfortable Wars: Toward a New Paradigm," *Parameters* 16, no. 4 (1986). Ernest Evans, "El Salvador's Lessons for Future U.S. Interventions," *World Affairs* 160, no. 2 (1997). Andrew Mack, "Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict," *World Politics* 27, no. 2 (1975). Michael Evans, "The 21st Century Security Environment," *The RUSI Journal* 154, no. 2 (2009). Ehsan Ehrari, "Transformation of America's Military and Asymmetric War," *Comparative Strategy* 29, no. 3 (2010). Michael Moodie, "Conflict Trends in the 21st Century," *Joint Forces Quarterly* (2009); Ralph Peters, "The Culture of Future Conflict," *Parameters* 25, no. 2 (1995); Daniel P. Bolger, "The Ghosts of Omduran," *Parameters* 21, no. 3 (1991); Vincent J. Goulding Jr., "Back to the Future with Asymmetric Warfare," *Parameters* 30, no. 4 (2000); Robert M. Cassidy, "Why Great Powers Fight Small Wars Badly," *Military Review* 82, no. 5 (2002).

[2] William B. Caldwell, IV, and Steven M. Leonard, "Field Manual 3-07. Stability Operations: Upshifting the Engine of Change," *Military Review*, 88 (July/August 2008). Department of the Army, Field Manual 3-24, *Counterinsurgency* (Washignton, Headquarters Department of the Army, 2006), 10-1, 1-28, 5-18.

[3] For more on metrics for success in counterinsurgency see: David Galula, *Counterinsurgency Warfare: Theory and Practice* (Westport, CT: Praeger Security International, 2006). David Killcullen, "Twenty-Eight Articles: Fundamentals of Company-level Counterinsurgency," *IO Sphere* (2006). Heather S. Gregg, "Beyond Population Engagement: Understanding Counterinsurgency," *Parameters* 39, no. 3 (2009). Bruce Hoffman, "Insurgency and Counterinsurgency in Iraq," *RAND* (2004). Colin Kahl, "Review: COIN of the Realm," *Foreign Affairs* 86, no. 6 (2007). Col. T.X. Hammes, "Insurgency: Modern Warfare Evolves into a Fourth Generation," *Institute for National Strategic Studies* 214(2005). Gregg, "Beyond Population Engagement: Understanding Counterinsurgency." Hoffman, "Insurgency and Counterinsurgency in Iraq." Kahl, "Review: COIN of the Realm." Hammes, "Insurgency: Modern Warfare Evolves into a Fourth Generation." Jacob N. Shapiro Luke N. Condra, "Who Takes the Blame? The Strategic Effects of Collateral Damage," *American Journal of Political Science* 56, no. 1 (2012). Stuart E. Johnson David C. Gompert, Martin C. Libicki, David R. Frelinger, John Gordon, IV, Raymond Smith, Camille A. Sawak, "Underkill: Scalable Capabilities for Military Operations Among Populations," *RAND Corporation* (2009).

[4] David A. Koplow, "Tangled Up In Khaki and Blue: Lethal and Non-Lethal Weapons In Recent Confrontations," *Georgetown Journal of International Law* 36, no. 3 (2005). David B. Law, "The US DoD's Next-Generation Non-Lethal Escalation-of-Force Weapons.," *Military Technology* 33, no. 5 (2009); Massimo Annati, "Non-Lethal Weapons Revisited," *Military Technology* 31, no. 3 (2007). Jesse. Kang Galvan, Theo, "The Future of the Army Nonlethal Scalable Effects Center," *Military Police* (2006). For a full history of modern non-lethal weapons see: Neil Davison, "The Early History of "Non-Lethal" Weapons," *Bradford Non-Lethal Weapons Research Project (BNLWRP)*(2006), http://www.bradford.ac.uk/acad/nlw/research_reports/docs/BNLWRP_OP1_Dec06.pdf; Neil Davison, "The Development of "Non-Lethal" Weapons During the 1990's.," *Bradford Non-Lethal Weapons Research Project (BNLWRP)*(2007), http://www.brad.ac.uk/acad/nlw/research_reports/docs/BNLWRP_OP2_Mar07.pdf; Neil Davison, "The Contemporary Development of "Non-Lethal" Weapons.," *Bradford Non-Lethal Weapons Research Project (BNLWRP)*(2007), http://www.brad.ac.uk/acad/nlw/research_reports/docs/BNLWRP_OP3_May07.pdf.

[5] MAJ Joe Schrantz,"The Long Range Acoustic Device: Don't Call It a Weapon-Them's Fightin' Words," *The Army Lawyer*, August 2010.

[6] For the only large scale independent review of ADS's health effects, see: Human Effects Advisory Panel, *A Narrative Summary and Independent Assessment of the Active Denial System* Penn State Applied Research Laboratory: 2008.

[7] For more on the LRAD, see: MAJ Joe Schrantz, "The Long Range Acoustic Device: Don't Call It a Weapon-Them's Fightin' Words," *The Army Lawyer* (2010); "LRAD Deters Birds for Aircraft, Airport Safety," *Air Safety Week* 25, no. 26 (2011); Jeremy Boren, "Safety of Long Range Acoustic Device debated," (Pittsburgh Tribune Review (PA), 2009); James Kraska and Brian Wilson, "Piracy Repression, Partnering and the Law," *Journal of Maritime Law & Commerce* 40, no. 1 (2009).

[8] Defense Science Board, "Defense Science Board Task Force on Directed Energy Weapons," ed. Department of Defense (2007).

[9] ADS's millimeter wave can penetrate clothing and glass, but not wood or metal. However, in testing, metal shields proved ineffective because the system works on any amount of exposed skin, however small. Even hiding behind concrete traffic barriers was ineffective because the beam came through the space been the road and the barrier. David A. Fulghum, "Silent Launch; New directed-energy weapon balances strength, low cost and portability," *Aviation Week and Space Technology* 165, no. 4 (2006).

[10] ACTD is a Department of Defense program for quickly moving promising new technologies into the hands of warfighters for evaluation.

[11] LTG Amos David GEN. David Petraeus, and LTC John Nagl, "Introduction," in *The U.S. Army-Marine Corps Counterinsurgency Manual* (Chicago: University of Chicago Press, 2007). For more on the history of ADS, see: Randy Roughton, "The Fast Goodbye," *Airman* 54, no. 4 (2010); "Raytheon Delivers Non-lethal Sheriff Active Denial System," *Microwave Journal* 48, no. 11 (2005); Alec Wilkinson, "NON-LETHAL FORCE," *The New Yorker* 2008; David Hambling, "Pain-inducing microwave weapon to fire from the sky," *New Scientist* 203, no. 2718 (2009); Nathan Hodge, "US commanders seek Active Denial System for use in Iraq," *Jane's Defence Weekly* 44, no. 44 (2007); John McHale, "Raytheon delivers Active Denial System 2 to U.S. Air Force," *Military and Aerospace Electronics* 8, no. 12 (2007); Tim Ripley, "USAF receives its second Active Denial System," *Jane's Defence Weekly* 44, no. 38 (2007). Amy Butler Sharon Weinburger, "A Sea of Pain," *Aviation Week and Space*

Technology 164, no. 14; John Dodge, "Military Beams over New Non-Lethal Weapon.," *Design News* 63, no. 7 (2008).

[12] For further media coverage on ADS' deployment and recall from Afghanistan, see: Ed Gumming, "The Weapon That's a Hot Topic," *The Daily Telegraph* 2010. Sean Hollister, "Raytheon's pain gun finally gets deployed in Afghanistan (update: recalled)," *Engadget*(2010). Noah Shachtman, "Pain Ray Recalled From Afghanistan," *Wired*(2010). David Hambling, "Army Orders Pain Ray Trucks; New Report Shows 'Potential for Death'," (2008). David Cairns, "US withdraws 'heat ray' gun from Afghanistan," *BBC*(2010). For more on the media reaction to the L.A. prison deployment see: Noah Shachtman, "Pain Ray, Rejected by the Military, Ready to Blast L.A. Prisoners," *Wired* (2010). Sharon Weinberger, "'Pain Beam' to Be Installed in LA Jail," *AOL News* (2010); Madalit Del Barco, "Zapping Inmates To Control Them: Harmless Or Torture?," *NPR*(2010). Thomas Watkins, "L.A. officials plan to use heat-beam ray in jail," *MSNBC* (2010). "An L.A. Jail's 'Excruciating' New Laser Weapon," *The Week*(2010). Torrance Stephens, "Los Angeles County Jail Uses Inmates as Test Rats for New Electronic Weapon," *Rolling Out*(2010). Ando Arike, "Rolling Back the Enlightenment: Pentagon "Pain Ray" to Debut in L.A.," *The Williamsburg Observer* (2010). Noah Shachtman "ACLU Blasts Jailhouse Pain Ray, Condemns 'Star Wars Tech'," *Wired*(2010). Clay Dillow, "L.A. Prison Using Experimental, Controversial 'Pain Ray' to Keep Inmates in Line" *PopSci*, August 24, 2010. "Prison to Use 'Excruciating' Pain Ray to Control Unruly Inmates," *The Daily Mail*, August 24, 2010.

[13] For more on general media coverage of the development of ADS, see: John Nolan, "Nonlethal heat-zapping weapon awaiting use," *The Journal-News* 2011. "US military unveils heat-ray gun ", *BBC*(2007). "US unveils ray beam as latest nonlethal weapon," *Korea Times* 2012. "State Of Active Denial," *Defense Technology International* 2007.

[14] For articles discussing ADS's ability to limit civilian deaths, see Dan Cairns, "US army heat ray gun in Afghanistan," *BBC*(2010). David Hambling, "Nervous Breakdown; Electromagnetic energy provides a way to harmlessly subdue troublemakers," *Defense Technology International* 2008. For articles discussing ADS use in crowd control, see Theunis Bates, "Shooting to Stun," *Time* 2007; Thomas Harding, "Non-lethal ray gun aims to quell rioters," *The Daily Telegraph* 2007. For articles discussing novel technical aspects of ADS, see Patrick Johnson, "How Hot is the Heat Ray Gun?," *BBC*(2007).

[15] For articles discussing the "science fiction" nature of ADS, see Ed Cumming, "The Active Denial System: the weapon that's a hot topic," *The Telegraph* 2010. Paul Koring, "Stranger than fiction: U.S. military unleashes its heat-ray weapon," *The Globe and the Mail* 341. and Philip Sherwell, "How I was zapped by US military's heat ray, that doesn't leave a mark Fiery blast is intended to show that weapon known as Silent Guardian is not dangerous," *The Sunday Telegraph* 2007. For articles concerned with foreign backlash, see "Active Denial System: Microwave Weapon Safe for Military Use? ," *International Business Times* 2012. Noah Shachtman, "U.S. Testing Pain Ray in Afghanistan ", *Wired*(2010). For articles concerned with the health effects of ADS, see Spencer Ackerman, "I Got Blasted by the Pentagon's Pain Ray — Twice," *Wired*(2012).

[16] In 2007, Human Rights Watch became one of the only organizations to do so when their Senior Military Analyst Marc Garlasco appeared on the *Democracy Now!* show to discuss the technology. He expressed support for the principle of non-lethal weapons, but highlighted a number of areas for concern. *Democracy Now*. "Pentagon Unveils Heat-Inducing Ray-Gun: Non-Lethal Crowd Control or Dangerous Weapon?" January 26, 2007. http://www.democracynow.org/2007/1/26/pentagon_unveils_heat_inducing_ray_gun.

[17] CED is the name for a class of weapons that use electric currents to disrupt muscle function and subdue potential belligerents. The best-known version of this weapon is manufactured by Taser International.

[18] Amnesty International, "Arming the Torturers: Electro-shock Torture and the Spread of Stun Technology," (Washington, D.C.: Amnesty International Press, 1997): 6-16; "US Authorities Urged to Control Tasers," Amnesty International, Press Release (May 27, 2011).

[19] Hugh Williamson, "Kazakhstan: Letter to the Prosecutor General regarding the December events in Zhanaozen and Shetpe," Human Rights Watch: February 1, 2012; Human Rights Watch, "China: Refrain From Using Excessive Force Against Protesters," New York: January 25, 2012; Jamie Fellner, "Letter to New York City Police Commissioner Raymond W. Kelly," January 28, 2004; Ken Roth, "Letter Regarding US Counterterrorism Assistance to Yemen," November 9, 2010; Human Rights Watch, "Uganda: Investigate Use of Lethal Force During Riots," Kampala: October 1, 2009.

[20] Kenneth Adams and Victoria Jennison, "What we do not know about police use of Tasers," *Int'l J. Police Strat. & Mgmt.* 30, no. 3 (2007): 452-453.

[21] *Democracy Now*. "Pentagon Unveils Heat-Inducing Ray-Gun: Non-Lethal Crowd Control or Dangerous Weapon?" January 26, 2007. http://www.democracynow.org/2007/1/26/pentagon_unveils_heat_inducing_ray_gun.

[22] The Special Rapporteur on the question of torture regularly releases interim reports, in accordance with the UN Commission on Human Rights' 1985 mandate for the position.
[23] Theo van Boven, "Report of the Special Rapporteur on the Question of Torture on the Trade and Production of Equipment Specifically Designed to Inflict Torture," United Nations Economic and Social Council Commission on Human Rights (Geneva: United Nations, 2004).
[24] This list included the United States on the basis that law enforcement officers had not used proper operating procedure when using conducted energy weapons. "Arming the Torturers: Electro-shock Torture and the Spread of Stun Technology," Amnesty International: (Washington, D.C.: Amnesty International Press, 1997): 6-16.
[25] Lennart Sjolberg, "Specifying factors in radiation risk perception," *Scandinavian Journal of Psychology* 41 (2000): 169-174.
[26] J. Bailer et al., "The relationship of worries about new technologies to environment related health complaints," *Zeitschrift Fur Klinische Psychologie Und Psychotherapie* 37, no. 1 (2008).
[27] G. J. Rubin, A. J. Cleare, and S. Wessely, "Psychological factors associated with self-reported sensitivity to mobile phones," *Journal of Psychosomatic Research* 64, no. 1 (2008).
[28] For further discussion of the psychological consequences of nuclear accidents, see F. N. von Hippel, "The radiological and psychological consequences of the Fukushima Daiichi accident," *Bulletin of the Atomic Scientists* 67, no. 5 (2011); N. V. Tarabrina, "Perception and Experiencing of "Invisible Stress" (in Relation to Radiation Incidents)," *Psychological Responses to the New Terrorism: A NATO-Russia Dialogue* 3, no. 1 (2005). E. J. Bromet and J. M. Havenaar, "Psychological and perceived health effects of the Chernobyl disaster: A 20-year review," *Health Physics* 93, no. 5 (2007).Kai Erikson, "Radiation's Lingering Dread," *Bulletin of the Atomic Scientists* (March 1991): 34-39.
[29] Kai Erikson, "Radiation's Lingering Dread," *Bulletin of the Atomic Scientists* (March 1991): 34-39.
[30] Depleted uranium (DU) was used by NATO forces in anti-tank weaponry during peacekeeping operations in the Balkans in the 1990's. NGOs, European scientific institutions, and the UN General Assembly all expressed fear that DU was harmful to local populations in the Balkans even after UN Environmental Programme studies showed that there was no health risk from DU. For further discussion of this topic, see Gustav Åkerblom, "Depleted Uranium—Experience of the United Nations Environmental Programme Missions," *AIP Conference Proceedings* 1034, no. 1 (2008).
[31] Human Effects Advisory Panel, "A Narrative Summary and Independent Assessment of the Active Denial System," (Penn State Applied Research Laboratory: February 11, 2008): 5.
[32] Lennart Sjolberg, "Specifying factors in radiation risk perception," *Scandinavian Journal of Psychology* 41 (2000): 173.
[33] For further discussion of this topic, see P. Slovic, "Perception of risk," *Science* 236: 280-285 and L. Sjoberg and E. Winroth, "Risk, moral value of actions, and mood," *Scandinavian Journal of Psychology* 27: 191—208.
[34] [awkward wording, redundant based on the body text] During the 1953 insurrection of Philippine Communists against the Philippine government, U.S. Air Force Colonel Edward Lansdale successfully frightened Huk guerrillas away from their strongholds by killing select insurgents as if *asuang*, or a local vampire, had murdered them near Huk territory. Superstition has also been used to unite local populations towards a common political cause. For example, insurgents against the European-educated Congolese political leadership in 1960 mobilized tribal populations against the government under the premise that the regime's attempts to ban witchcraft were themselves evil acts of sorcery. Similarly, since the 1980's, Maoist insurgents in the rural Indian province of Maharashtra have convinced local residents that the police ban on superstitious practices is to blame for misfortunes in towns like Bodalkasa, which suffers from an unusually high adolescent death rate. John J. Tierney Jr, "Can a Popular Insurgency Be Defeated?," *Military History* 24, no. 1 (2007).Price and James R. Price and Paul Jureidini, "Witchcraft, Sorcery, Magic, and other Psychological Phenomena and their Implications on Military and Paramilitary Operations in the Congo," (Washington, D.C. : Special Operations Research Office, 1964). 1964; and Amit Desai, "Anti-'anti-witchcraft' and the Maoist insurgency in rural Maharashtra, India," *Dialectical Anthropology* 33, no. 3/4 (2009).
[35] Hafizullah Emadi, *Culture and Customs of Afghanistan* (Westport, CT: Greenwood Press, 2005): 63.
[36] In 2008, The RAND Corporation hosted a discussion among experts on Arab and Muslim population about different aspects of a continuum of force. These experts indicated that "an unfamiliar effect from what may seem a mysterious device could cause great consternation, abundant rumors, and lasting suspicions that ailments are the result of that device." For more discussion of this topic, see Stuart E. Johnson David C. Gompert, et. al. , "Underkill: Scalable Capabilities for Military Operations among Populations," (Arlington, VA: RAND Corporation, 2009).

[37] Jerome D. Frank, "Nuclear Arms and Nuclear Leaders": Sociopsychological Aspects of the Nuclear Arms Race," *Political Psychology* 4, no. 2 (June 1983): 393-408.
[38] Sjef Orbons, "Do Non-Lethal Capabilities License to 'Silence'?" *Journal of Military Ethics* 9, no. 1 (2010): 78-99.
[39] Chris Mayer, "Nonlethal weapons and noncombatant immunity: is it permissible to target noncombatants?" *Journal of Military Ethics* 6, no. 3 (2007): 221-231; and P. Kaurin, *With Fear and Trembling: A Qualified Defense of 'Non-Lethal' Weapons* (Tacoma, Pacific Lutheran University: 2008).
[40] Christian Enemark, "'Non-lethal' weapons and the occupation of Iraq: technology, ethics, and law," *Cambridge Review of International Affairs* 21, no. 2 (2008): 200.
[41] Christian Enemark, "'Non-lethal' weapons and the occupation of Iraq: technology, ethics, and law," *Cambridge Review of International Affairs* 21, no. 2 (2008): 201.

[42] David P. Fidler, "The Meaning of Moscow: 'Non-Lethal Weapons' and International Law in the 21st Century, " *International Review of the Red Cross* 87, no. 859 (September 2005).
[43] Defense Acquisition University. "Question and Answer Detail" Available online at: https://dap.dau.mil/aap/pages/qdetails.aspx?cgiSubjectAreaID=38&cgiQuestionID=106517
[44] Hambling, David. "Pain Ray First Commercial Sale Looms", *Wired,* August 5, 2009. Defense Security Cooperation Agency "The FMS Advantage: Frequently Asked Questions About Foreign Military Sales"
[45] http://www.taser.com/products/on-officer-video/taser-axon
[46] In fact, some form of recording system is already in place on the prototypes of ADS available to the military, although the chain of command associated with these recordings and the measures put in place to prevent tampering are not publicly available.
[47] For examples of successful TASER protocols in various police departments throughout the United States, refer to Robert J. Cramer, "Taser Weapons: Use of Tasers by Selected Law Enforcement Agencies: GAO-05-464," (U.S. Government Accountability Office, 2005).
[48] Miller: 30-31, 143-146.
[49] For example, operational and tactical doctrines will vary significantly depending on whether the deployment is domestic or international, controlled by police forces or by military units, and whether it is deployed on land or at sea.
[50] Police officers are often fired when it has been confirmed that they used their TASER in an inappropriate manner, such as on a restrained target or on a target's neck. For examples of such incidents, see "Two Rockingham police officers were yesterday sacked for repeatedly misleading investigators during the inquiry into the misuse of Tasers on other officers at the station," (Y, 2010); Press The Associated [is that how you actually cite that?], "Evergreen, Ala. police officer fired," (The Associated Press, 2011); Matt McKinney, "Mpls. cop fired over Taser arrest wants his job back: The officer contends the department's probe into the incident had a predetermined outcome to silence criticism," (Star Tribune (Minneapolis, MN), 2010).
[51] J. Strote and H. Range Hutson, "Taser use in restraint-related deaths," *Prehospital Emergency Care* 10, no. 4 (2006).
[52] US Department of Defense Non-Lethal Weapons Program. *Non-Lethal Weapons for Today's Operations.* (Washington: DOD, 2010), 9.
[53] While Area Defense System would allow ADS to keep the same acronym, there is already a technology in development called the High Energy Liquid Laser Area Defense System (HELLADS) which could potentially cause confusion.
[54] David C. Gompert, "Underkill: Scalable Capabilities for Military Operations Among Populations."
[55] John Bartus, "Tasers: Peaceful for Police, Safer for Subjects" *Keysweekly.com* 17 July 2009 http://keysweekly.com/42/tasers-peaceful-for-police-safer-for-subjects/ (18 December, 2011) – The use of demonstrations by the Orlando Police Department was also discussed in Miller.

A New "Freedom" Fighter: Building on the T-X Competition

Peter Klicker

The development and deployment of state-of-the-art fighter aircraft gives the United States dominance in the air but prevents the U.S. government and aerospace industry from fulfilling the demand of less advanced foreign air forces for low-cost jet fighters. China, in contrast, has succeeded in this market segment for decades and will further its competitive posture in the years to come. U.S. efforts to fill this fighter gap, through the Light Air Support (LAS) program, have focused on identifying a turboprop aircraft for close air support or counterinsurgency (COIN) operations. Many air forces, however, have been reluctant to spend scarce resources on armed turboprops, which they view as having limited capability.

This brief proposes that the U.S. Air Force (USAF) instead capitalize on the existing T-X competition, which seeks a replacement for T-38 training jets, to develop a low-cost fighter for export. During the Cold War, the United States sold a significant number of militarized jet trainers, such as the F-5 and the A-37, to partners in the developing world. The practice of turning a jet trainer into a low-cost, easily maintained fighter was a success and should be revived. This program will allow the United States to strengthen its joint military efforts with partner states, bolster its aerospace industry, and counter rising Chinese influence.

Current Status of Fighter Jet Sales

The superiority of U.S. fighter aircraft makes them an attractive purchase for air forces throughout world. However, not all U.S. partners can afford such advanced aircraft or possess the resources and skill level needed to operate and maintain them. These states instead seek the kind of low-cost, yet capable, fighter aircraft that China has sold for decades. Without change, the United States risks falling further behind China in this market segment.

Comparison of U.S. and Chinese Fighter Jet Sales

Since the end of the Cold War, total U.S. fighter jet sales have exceeded Chinese sales by a margin of nearly 2,000 aircraft.[1] However, during that same time period, China received nearly three times as many orders for low-cost fighters as the United States.[2] The gap between the two countries has continued to widen. Between 2000 and 2010 China sold 312 low-cost fighters whereas the United States exported only ten.[3]

Since the end of the Cold War, China has sold aircraft to a greater number of states and in a wider variety of regions. Beijing has exported variants of four fighter models to fifteen states in Africa, Southern Asia, South-Eastern Asia, and South America.[4] With the K-8, for example, China broke into the Latin American market and increased its sales in Africa.[5] Chinese fighter jets also have increased in quality. China has progressed from copying Soviet aircraft, such as the MiG series, to producing indigenously designed aircraft like the K-8 and JF-17.[6]

Future Trends in the Chinese Aerospace Industry

Aviation Industry Corporation of China (AVIC), China's state-owned aerospace company, and its export arm, China Aero-Technology Import Export Corporation (CATIC), are taking several steps to strengthen China's competitive posture in the aerospace industry.

- *Development*:
  - China has developed rapid prototyping production centers modeled on Lockheed Martin's Skunk Works and Boeing's Phantom Works projects.[7]
  - AVIC intends to invest $1.35 billion into jet engine research and development over the next five years. Through this investment, AVIC aims to free China of its dependence on Russian technology and expand Chinese aircraft exports.[8]
- *Export*:
  - AVIC seeks to increase the quality and sophistication of Chinese military aircraft, with the aim of exporting to a wider variety of states, particularly in emerging markets in Africa and Asia.[9]
  - CATIC had made the affordability of Chinese military aircraft, relative to western aircraft, a central aspect of its export strategy.[10]
- *Training, Maintenance, and Post-Sale Support*: China places increasing emphasis on customer service and post-sale support for military equipment customers.[11] According to AVIC reports, China maintains support offices and overseas companies in 12 African states. China also operates 14 military attaché offices in Africa. Five of those offices are located in states that have purchased Chinese fighter jet aircraft.[12]

Implications of U.S. Fighter Jet Sales

Fighter jet sales produce long-term payoffs that extend beyond the initial transaction. Specifically, fighter jet exports contribute to U.S. political, military, and economic power. Both the U.S. aerospace industry and the country as a whole benefit from these sales.

Political

Fighter jet sales foster closer political-military relationships between the United States and partner states by providing the resources needed to achieve mutual security goals.

- *U.S. Foreign Policy Strategy*: Both the 2010 National Security Strategy (NSS) and the 2010 Quadrennial Diplomacy and Development Review (QDDR) emphasize investment in partner capacity as a means of increasing security burden sharing.[13]

- *Foreign Military Sales (FMS)*: The FMS program strengthens U.S. national security by enhancing the defense capabilities of U.S. partners, which allows those states to better provide for their own defense and to contribute to regional and global security. FMS also increases U.S. leverage in its relationships with purchasing states.[14]

Military

Fighter jet sales advance U.S. defense policy by fostering and sustaining military-military relations with other states, primarily through joint-training exercises. Many states choose to buy U.S. military hardware due to superior post-sale support and the opportunity to develop military-military relations. China has taken note and is increasing its efforts in these areas.

- *Joint Training*: The 2010 Quadrennial Defense Review (QDR) recommends improving upon existing efforts to strengthen the defense capacities of partner states through joint-training.[15] According to the QDR, the USAF currently only meets half of the demand for training partner aviation forces. In response, the Air Force intends to field more light mobility and light attack aircraft for training purposes.[16]

- *Partner Capacity*: The Defense Department's 2012 Strategic Guidance emphasizes investing in partner capacity.[17] Notably, the report also states that the U.S. military will rebalance toward the Asia-Pacific, China's main sphere of influence.[18] Further, the United States will "seek to be the security partner of choice" and pursue new partnerships in Africa and Latin America, where China is also active.[19]

- *Interoperability*: According to the Defense Security Cooperation Agency, which coordinates military exports for the Defense Department, FMS contributes to coalition building and the strengthening of bilateral military relations by enhancing interoperability between U.S. and partner forces.[20]

Economic

Fighter sales create jobs for the U.S. aerospace industry and lead to the purchase of other military equipment.

- *Aerospace Industry and Job Creation*: The aerospace industry is a significant source of domestic job creation and also contributes positively to the U.S. economy as a

whole. In 2011 aerospace industry exports contributed $87 billion to the domestic economy. Aerospace also boasts the largest positive trade balance ($57.4 billion) of any U.S. manufacturing industry.[21]

- *Further Military Hardware Sales*: Purchasers of U.S. fighter jets often buy other military hardware as well, such as missiles, parts, and equipment.[22] These additional sales help to extend production lines and lower unit costs.

Looking to the Past: Historical Models for Fighter Aircraft Sales

During the Cold War, the United States undertook several efforts to equip its partners with low-cost but capable aircraft. During the Vietnam War, the United States used jet aircraft as well as piston-powered and turboprop aircraft, such as the A-1 and OV-10. In a second and more general historical model, the United States exported low-cost fighter jets, such as the F-5 and A-37, to partners throughout the world. Many of these aircraft sales took place under the auspices of the Military Assistance Program (MAP), which sought to check Soviet aggression by providing the armed forces of friendly states with military hardware and training programs.[23] Examining these two historical models—turboprops versus fighter jets—will help identify the best path forward.

Use of Prop-Driven Aircraft during the Vietnam War

During the Vietnam War, the United States flew aircraft like the Douglas A-1 Skyraider and the Rockwell OV-10 Bronco for its own combat missions. It also provided A-1s directly to the South Vietnam Air Force (VNAF).[24]

- *A-1 Skyraider*: The USAF initially used the piston-powered Skyraider to train and equip the VNAF's fighter squadrons.[25] In later years the Air Force used the A-1 for its own combat missions in Vietnam. The Skyraider provided close air support and also served in search and air rescue missions.[26]

- *OV-10 Bronco*: The turboprop OV-10 primarily served as a forward air control aircraft in Vietnam. The Bronco was capable of taking off in short spaces and rough terrain, which allowed it to better support troops in forward areas.[27]

Cold War Fighter Jet Sales

The simultaneous development of the T-38 trainer and F-5 fighter as well as the T-37 trainer and A-37 fighter demonstrated the effectiveness of turning a trainer aircraft into a light fighter for export.

- *T-38 and F-5*

    - The T-38 and F-5 were both developed from Northrop's privately-funded N-156 lightweight fighter project.[28] Northrop designed the aircraft for U.S. partners who wanted a low-cost alternative to more advanced U.S. fighter aircraft. The U.S. military initially rejected the fighter version of the aircraft but did select the trainer version, re-designating it the T-38 Talon.[29] The USAF later chose the fighter version to supply foreign air forces under MAP, re-designating the aircraft the F-5 Freedom Fighter.[30]

    - The F-5 went on to great success as an export aircraft—over 2,300 were sold—and remains the ninth most active combat aircraft in the world.[31] F-5 sales benefited from the active support of the Air Force, which used the aircraft operationally in Vietnam and offered joint-training programs with purchasing air forces. The T-38 also remains in service, primarily with the USAF.[32]

- *T-37 and A-37*:

    - The Cessna T-37 Tweet initially entered USAF service as a training aircraft.[33] The Air Force later contracted Cessna to modify the T-37 into an attack variant, the A-37 Dragonfly, to replace its aging fleet of A-1 Skyraiders.[34] The A-37s took over the missions in Vietnam previously carried out by prop-driven aircraft.[35]

    - The A-37 also achieved success as an export aircraft—over 500 were sold—and is still operated today, as is the T-37.[36] As with the F-5, active USAF support facilitated the export of A-37s and T-37s and strengthened military-military relations through joint training.

Borrowing from the Past: Developing the New 'Freedom' Fighter

The remainder of the brief examines two paths forward for the Air Force in its mission to develop a low-cost fighter for export to partner states. The first option is to continue the development of a turboprop aircraft through the Light Air Support (LAS) program. The second option is to repurpose the T-X competition to include the development of a low-cost fighter jet variant, similar to the F-5 and A-37. This brief recommends the second option.

Option #1: Turboprop Aircraft and the LAS Program

The LAS program is designed to provide Afghanistan with an armed turboprop aircraft for light attack, reconnaissance, and COIN missions. The aircraft will fulfill a role similar to that of the A-1 Skyraider and OV-10 Bronco during the Vietnam War. The USAF will select the aircraft and then train the Afghani Air Force to operate it.

- *Origins of LAS*: The LAS program originated in the Air Force's desire for a Light Attack/Armed Reconnaissance (LAAR) aircraft, intended for export and dedicated to COIN and irregular warfare missions.[37] In 2010 LAAR was subsumed into LAS.[38]

- *Aircraft under Consideration for LAS*: The two aircraft under consideration for LAS are the Hawker Beechcraft AT-6 and the Embraer A-29 Super Tucano.

    - The Hawker Beechraft AT-6 is a light attack variant of the T-6 Texan II turboprop trainer used by the U.S. Navy and the USAF.[39]

    - The Embraer Super Tucano, or A-29, is a Brazilian aircraft that currently serves with five world air forces. It functions primarily as a COIN aircraft in rugged terrain environments.[40]

- *Current State of LAS*: The USAF awarded the LAS contract to Embraer in December 2011 but issued a stop-work order in January 2012 pending litigation by Hawker Beechcraft, which believes it was unfairly excluded from the competition.[41] The Air Force cancelled the contract in February 2012 and is due to issue a modified request for proposals in April 2012.[42]

Limitations of the LAS Program

The LAS program has some advantages. Turboprops cost less than jets to purchase and are cheaper and easier to maintain. Most air forces can operate them.[43] They perform well in rugged terrain and with relatively short runways, and can be stationed closer than jets to troops as a result. Turboprops can also loiter in the air longer and at a lower cost than jets. However, the LAS program has a number of significant drawbacks.

- Most air forces have no desire to operate turboprops, as they are perceived as less capable—in large part because they are not used in combat by the USAF.[44]

- Given the current fiscal situation, it is unlikely that the USAF will expand its order beyond the 20 aircraft needed for the Afghan Air Force. With no further sales on the horizon, LAS cannot serve as an effective means for building partnership capacity.

- Congress has been skeptical of efforts to field LAS type aircraft.[45] Possible reasons for this skepticism include disagreements over the aircraft to be used and lack of effective advocacy on the part of the Air Force.[46] Questions have also been raised about the viability of the long-term U.S.-Afghani relationship.[47]

- Unlike more versatile jet aircraft, turboprops are effectively limited to light air-to-ground and close air support missions. This limited capability reduces the number of threats to which they can respond.

- Turboprops lack the speed of jets and are less able to get to needed locations quickly and to transit danger zones.

Option #2: Fighter Jets and the T-X Competition

The T-X competition will identify a replacement for the USAF's aging fleet of T-38 trainer aircraft. The T-38s have an average age of 43.5 years and need to be replaced given safety concerns and because their dated technology is inadequate for training pilots to fly fifth generations fighters, such as the F-22 and F-35. In addition to selecting a replacement for the T-38, the Air Force should also view T-X as an opportunity to acquire a light attack fighter for export.

- *Overview of T-X*

  - Air Education and Training Command (AETC) began the acquisition process to replace the T-38 in 2003.[48] The Air Force intends to procure 350 new trainers, but with naval and light attack versions, the U.S. order could reach nearly 1,000 aircraft.[49] The USAF plans to award the contract in FY2016 and operationalize the T-X fleet in 2020.[50]

  - The Air Force is seeking a low-cost, two-seat military jet trainer aircraft and ground-based training systems.[51]

  - The (FY) 2012 budget requests $300 million for a three year engineering, manufacturing, and development (EMD) phase. Given that level of funding, the USAF's current option is to select an off-the-shelf design.[52]

- *Aircraft under Consideration*: The three aircraft receiving the most attention are foreign, off-the-shelf designs.

  - Alenia Aermacchi M-346: Alenia Aeronautica expects to rebrand its twin-engine M-346 trainer as the T-100 and offer it for the T-X competition.[53]

  - BAE Systems Hawk: BAE Systems has partnered with Northrop Grumman Technical Services to offer the Hawk Advanced Jet Training System (AJTS).[54] AJTS includes the Hawk T2 aircraft and on-the-ground simulators.[55]

  - Korea Aerospace Industries (KAI)/Lockheed Martin T-50 Golden Eagle: Lockheed Martin and KAI plan to offer their T-50 Golden Eagle trainer aircraft, which was designed with the eventual replacement of the T-38 in mind.[56]

  - Boeing: Unlike the other potential bidders, Boeing is considering developing a clean-sheet design that would be purpose built for T-X.[57]

- *Concept of Operations*: The fighter variant of the T-X trainer aircraft would fill a light-to-medium attack and limited air defense role.[58]

- *Potential Market*: The aircraft can be marketed both to areas where China sells low-cost jets and to areas where the planes contending for T-X have already been sold.

    - China has sold comparable aircraft, such as the K-8, to states in Africa (Egypt, Ghana, Namibia, Sudan, Tanzania, Zambia, and Zimbabwe), Southern Asia (Sri Lanka), South-Eastern Asia (Myanmar), and South America (Venezuela and Bolivia).[59] While many of the above would not purchase U.S. aircraft for political reasons, they represent the kind of air forces interested in acquiring this capability.

    - BAE has sold the Hawk T2 to Australia, Bahrain, Canada, India, and the United Kingdom.[60] KAI has sold the T-50 to Indonesia, and the Philippines has taken the aircraft under consideration.[61] Alenia has sold the M-346 to Singapore.[62]

<u>Strengths of the T-X Approach</u>

- The USAF needs to replace the T-38s given concerns over the safety of their continued operation and their inability to adequately train F-22 and F-35 pilots.[63]

- The strategy of turning a jet trainer into a light air sovereignty and attack fighter has worked well in the past, as demonstrated by the F-5 and the A-37.

- Many of the aircraft under consideration for T-X already have the capability to serve as a trainer and a light fighter.

- The development of a fighter version for export would extend the production line for the T-X winner, lowering the unit cost and creating domestic jobs.

- The off-the-shelf nature of the aircraft would minimize concerns over end-use agreements and the sharing of advanced proprietary technology.

- U.S. operation of the trainer version would increase the likelihood of foreign purchases of the fighter version.[64]

- Politically and militarily, the United States would benefit from acquiring an aircraft with which to build partnership capacity and facilitate interoperability in the developing world

Possible Objections

- In the current budgetary environment, the Air Force may be unwilling to invest heavily in developing partner capacity.

  Response: Investing in partner capacity is a central aspect of several strategy documents, including the most recent NSS, QDR, QDDR, and USAF Global Partnerships Strategy. This proposal offers a concrete way to make that idea a reality, while capitalizing on a pre-existing and much needed program to replace the T-38.

- In the current business environment and given the failure of the Northrop F-20 (a 1980s era lightweight fighter project), aerospace companies may be reluctant to invest in a new lightweight fighter without the explicit Air Force support.[65]

  Response: The F-20 failed in large part due to disagreements and miscommunications between Northrop and the U.S. government. This proposal recommends that the USAF make the development of a fighter variant an explicit component of T-X.

- As the United States and its allies transition to fifth generation fighters, increasing quantities of used F-16s will come onto the market. Many air forces would rather fly a well-regarded aircraft long operated by the United States than take a risk on a new lightweight fighter.[66]

  Response: The nearly 40-year-old F-16 is entering the end of its life cycle. Production has slowed and there are few potential new buyers.[67] Most of the F-16s sold in the past decade were replenishment aircraft for states that already operate the F-16.[68] The aircraft under consideration for T-X would be cheaper than a new F-16 and most likely cheaper than a used F-16.[69]

  An armed T-X can constitute the low-end of a high-low technological mix in a developing air force with a limited budget. Fighter variants of the T-X can specialize in light-to-medium ground support, limited air sovereignty, and aircrew training. F-16s can be used for more demanding mission profiles.[70]

- Air forces never prioritize trainer acquisitions, and the demand for turbine powered trainers, which has shrunk in recent years, is projected to remain flat until 2020.[71]

  Response: The T-X program is a medium-term investment with initial operating capability slated for 2020. Several factors could contribute to a resurgence in international demand by that year. First, states will have more fully recovered from the economic recession and have a better sense of their defense budgets. Second, aging Cold War era aircraft like the F-5 and A-37 will soon need to be retired and replaced. Third, there would be an opening for a new cost-effective fighter when the F-16 production line closes, as not all states can transition to the F-35.[72]

Conclusion

Although armed turboprop aircraft are well suited for some missions, they are of little interest to most air forces. Given this reality and mounting congressional opposition, the Air Force should abandon further development of the LAS program. To fill the light fighter gap, the Air Force should instead re-envision the T-X competition as a means to acquire both a new jet trainer and a light attack variant aircraft for export. This approach worked well in the past and should be revived today. Enacting this proposal will allow the United States to enhance its political-military relationships, bolster its aerospace industry, and counter rising Chinese influence.

This proposal is within the reach of the United States and offers a large, long-term pay-off for a relatively small, medium-term investment. While the U.S. military and the U.S. aerospace industry now operate in a more challenging fiscal environment, they can and should work together to advance U.S. security goals. This proposal offers a concrete means to advance U.S. national security by expanding the T-X competition to include acquiring a light fighter for export—the New "Freedom" Fighter.

---

[1] SIPRI Arms Transfers Database (Stockholm International Peace Research Institute), s.v. "USA: Transfers of major conventional weapons: sorted by recipient. Deals with deliveries or orders made for year range 1950 to 2010," December 16, 2011. "Fighter-type" aircraft in this analysis include those weapons designated in the SIPRI database as "Fighter aircraft," "FGA aircraft" (Fighter/ground attack aircraft), and "Trainer/combat ac" (training aircraft with light attack capabilities); Ibid., s.v. "China: Transfers of major convention weapons: sorted by recipient. Deals with deliveries or orders made for year range 1950 to 2010," December 16, 2011. From 1991 to 2010 the United States received orders for 2,469 fighter-type aircraft and China received orders for 590 such planes.

[2] Ibid. "Low-cost, low-end fighter-type aircraft" are comparable to the F-5 Freedom Fighter in its day, and below the cost/capability levels of fourth and fifth generation aircraft such as the F-16, F/A-18, F-15, F-35, and AV-8B Harrier II. While all 590 of the Chinese exports were of the low-cost variant, the United States only exported 213 such planes.

[3] Ibid., "USA."; Ibid., "China."

[4] Ibid., "China."; "United Nations Statistics Division: Standard Country and Area Codes Classification." United Nations, September 20, 2011, http://unstats.un.org/unsd/methods/m49/m49regin.htm.

[5] SIPRI., "China."

[6] The K-8 and the JF-17 are both joint efforts of China and Pakistan. The K-8 is a lightweight jet aircraft that serves both as a pilot trainer and light striker fighter. The JF-17 is a lightweight multi-role fighter that is intended to compete with the F-16 in the export market; Gabe Collins and Andrew Erickson, "Jet Engine Development in China: Indigenous high-performance turbofans are a final step toward fully independent fighter production," China SignPost, June 26 2011, http://www.chinasignpost.com/2011/06/jet-engine-development-in-china-indigenous-high-performance-turbofans-are-a-final-step-toward-fully-independent-fighter-production/. China's inability to domestically mass-produce jet engines at consistently high quality levels has limited the growth of the state's aerospace industry.

[7] Bradley Perrett, "Avic Defense Adopting Skunk Works Model," *Aviation Week*, January 14, 2011, http://www.aviationweek.com/aw/generic/story.jsp?id=news/asd/2011/01/14/01.xml&channel=misc

[8] Gabe Collins and Andrew Erickson, "Jet Engine Development in China."

[9] Wendell Minnick, "China Leaps Into Global Aircraft Market," DefenseNews, November 23, 2009, http://minnickarticles.blogspot.com/2009/11/china-leaps-into-global-aircraft-market.htm. For decades, many Chinese fighter jet sales have been to "pariah" states such as Iran, Myanmar, Sudan, and Zimbabwe, which were unable to buy elsewhere due to arms and trade sanctions; Sale at Dubai Air Show: 3 JF-17 Thunders for a price of a F-16," Rupee News, November 13, 2011, http://rupeenews.com/2011/11/sale-at-dubai-air-show-3-jf-17-thunders-for-a-price-of-a-f-16/.

[10] Reuben Johnson, "China's CATIC/AVIC Offering New Full-Spectrum Flight Training System," *Aviation Week*, January 31, 2010, http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=busav&id=news/CATIC013110.xml; Siva Govindasamy, "China's AVIC steps up sales push for FC-1, J-10 fighters," Flightglobal, September 30, 2009, http://www.flightglobal.com/news/articles/chinas-avic-steps-up-sales-push-for-fc-1-j-10-fighters-332905/. Specifically, CATIC intends to aggressively market the J-10 and JF-17 to states seeking to modernize their fleets but unwilling or unable to pay for western fourth or fifth generation jet aircraft.
[11] Reuben Johnson, "This Is Not The Last Chinese Aircraft We Will Buy: Pakistan," *Aviation Week*, July 22, 2010, http://www.aviationweek.com/aw/generic/story.jsp?id=news/awx/2010/07/22/awx_07_22_2010_p0-242943.xml&channel=defense.
[12] Kent Hughes Butts and Brent Bankus, "China's Pursuit of Africa's Natural Resources," U.S. Army War College Center for Strategic Leadership, June 2009, http://www.csl.army.mil/usacsl/publications/CCS1_09_ChinasPursuitofAfricasNaturalResources.pdf. Those five states are Nigeria, Namibia, Sudan, Zambia, and Zimbabwe.
[13] "National Security Strategy," White House, May 2010, 11, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf; "Quadrennial Diplomacy and Development Review," U.S. Department of State, 2010, http://www.state.gov/documents/organization/153108.pdf.
[14] Robert N. Peterman, *Fighter Aircraft Foreign Military Sales: Industry Survival and National Power*, 1993, 1, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA276788.
[15] "Quadrennial Defense Review," U.S. Department of Defense, February 2010, 49, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf.
[16] Ibid., 53.
[17] "Sustaining U.S. Global Leadership: Priorities for 21st Century Defense," U.S. Department of Defense, January 2012, 9, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf.
[18] Ibid., 8.
[19] Ibid., 9.
[20] "ForeignMilitarySales," DefenseSecurityCooperationAgency, http://www.dsca.osd.mil/home/foreign_military_sales.htm; Carter Ham (discussion, Defense Writers Group, Washington, D.C., September 14, 2011), U.S. Africa Command, http://www.africom.mil/getarticle.asp?art=7205. General Carter Ham, Commander, U.S. AFRICOM, has stated that while he does not view Chinese military sales in Africa as a competition between the United States and China, he would prefer that African states purchase U.S. equipment, as it would facilitate joint-training and strengthen military-military relations.
[21] Aerospace Industries Association, *2011 Year-End Review and Forecast*, http://www.aia-aerospace.org/assets/YE_Analysis.pdf.
[22] "Morocco – AIM-9X-2 SIDEWINDER Missiles," Defense Security Cooperation Agency, May 18, 2011, http://www.dsca.mil/pressreleases/36-b/2011/Morocco_11-01.pdf. For example, two years after Morocco reached an agreement with the United States to purchase F-16s, the DCSA notified Congress of a possible $50 million FMS package to Morocco consisting of Sidewinder missiles, as well as associated equipment, parts, training and logistical support.
[23] Donald F. Blake, "A Realistic Look at USAF Military Assistance and Foreign Military Sales," Air University Review (November-December 1970), http://www.airpower.au.af.mil/airchronicles/aureview/1970/nov-dec/blake.html. The Military Assistance Program (MAP) fit into a broader U.S. effort during the Cold War to check Soviet expansion by fostering political, economic, and military relationships with allied and partner states. In particular, MAP sought to strengthen the armed forces of friendly states by providing them with military hardware and training programs. In regard to aircraft, between 1950 and 1970 the USAF provided or programmed approximately 16,750 aircraft, such as the F-5 Freedom Fighter, to 55 states.
[24] Jane's International Defense Review: IDR., Volume 41, Jane's Information Group, 2008, http://books.google.com/books?ei=zvAVT4_3NKjv0gG6j82BAw&id=e2I-AQAAIAAJ&dq=turboprops+in+vietnam&q=%22during+the+vietnam+war%22#search_anchor.
[25] "Douglas A-1E Skyraider," National Museum of the U.S. Air Force, February 15, 2011, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=297.
[26] Ibid.
[27] E. Burrows, "Legends of Vietnam: Bronco's Tale," *Air and Space*, March 2010, 4, http://www.airspacemag.com/military-aviation/Legends-of-Vietnam-Broncos-Tale.html?c=y&page=4.

[28] Anthony Tambini, *F-5 Tigers over Vietnam* (Boston: Branden, 2001), 8. Northrop initiated the project after discovering that many NATO and SEATO allies could not utilize existing U.S. fighters and desired an affordable and easily-maintained multi-role fighter.
[29] Jerry Scutts, *Northrop F-5/F-20* (London: Ian Allan, 1986), 8.
[30] F.G. Swanborough, *United States Military Aircraft Since 1909* (London: Putnam, 1963), 396-7.
[31] SIPRI, "USA."; Flightglobal Insight, *World Air Forces 2011/2012*, 8, http://www.flightglobal.com/airspace/media/reports_pdf/emptys/90190/world-air-forces-2011-2012.pdf. As of 2011, 518 F-5 remain in service with 23 world air forces.
[32] Ibid. As of 2011, 564 T-38 remain in service with two world air forces. The majority are operated by the USAF.
[33] 'Cessna T-37B Tweet," National Museum of the U.S. Air Force, October 11, 2007, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=381. In 1959 a more powerful and advanced version of the T-37, the T-37B, entered service. An export version of the T-37, the T-37C, was also developed with provisions for armament and extra fuel.
[34] "Cessna A-37 Dragonfly," National Museum of the U.S. Air Force, February 15, 2011, http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=326. After the successful performance of the A-37As in Southeast Asia, the USAF ordered newly built A-37Bs which included further improvements in power, armament, and fuel capacity.
[35] Kev Darling, *Tweet and the Dragonfly: the Story of the Cessna A-37 and T-37* (Lulu.com, 2005), 19.
[36] SIPRI, "USA." The A-37 sold particularly well in Latin America. Purchasers included Chile, Colombia, the Dominican Republic, Ecuador, El Salvador, Guatemala, Honduras, Peru, and Uruguay. It was also sold to states in Asia such as South Korea, South Vietnam, and Thailand; Flightglobal Insight, *World Air Forces*. As of 2011, 58 A-37 aircraft remain in service with six world air forces. Similarly, 118 T-37 aircraft remain in service with five world air forces.
[37] "Air Combat Command (ACC) Light Attack/Armed Reconnaissance (LAAR)," U.S. Air Force, July 27, 2009, https://www.fbo.gov/index?print_preview=1&s=opportunity&mode=form&id=b30065477e7b9159bb2687f2cc2a3667&tab=core&tabmode=list. In 2009 the USAF issued a request for information (RFI) detailing the requirements for a LAAR aircraft to be supplied to Air Combat Command (ACC) starting in (FY) 2012.
[38] Graham Warwick and Bill Sweetman, "U.S. Wants COIN Aircraft For Foreign Training," *Aviation Week*, April 20, 2011, http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/dti/2011/04/01/DT_04_01_2011_p38-297236.xml. Specifically, the LAS program aims to procure 20 aircraft for the Afghan Air Force and an additional 15 aircraft to meet USAF's requirement for a LAAR aircraft with which to build partner capacity. Delivery of aircraft to Afghanistan was originally scheduled to begin in April 2013, but that date will likely be pushed back due to litigation issues surrounding the contract.
[39]Warwick and Sweetman, "U.S. Wants COIN Aircraft." In addition to its armament, the AT-6 includes an integrated surveillance/attack mission system supplied by Lockheed Martin as well as an upgraded avionics package based on the A-10C.
[40]"A-29 Super Tucano Wins Defense Contract in U.S.," Embraer, December 30, 2011, http://www.embraer.com/en-US/ImprensaEventos/Press-releases/noticias/Pages/SUPER-TUCANO-VENCE-CONTRATO-DE-DEFESA-NOS-EUA.aspx. The A-29 was originally designed to fulfill the Brazilian Air Force's requirement for a light-attack/advanced-trainer aircraft.
[41] Molly McMillin, "Air Force Temporarily Halts Contract After Hawker Beechcraft Suit," *Wichita Eagle*, January 5, 2012, http://www.kansas.com/2012/01/05/2163375/air-force-temporarily-halts-contract.html.
[42] Andrea Shalal-Esa, "Air Force scraps deal with Embraer, Sierra Nevada," Reuters, 28 February 2012, http://www.reuters.com/article/2012/02/29/us-embraer-snc-aircraft-idUSTRE81R1W920120229; Amy Butler, "USAF Crafts New Light Air Support RFP," Aviation Week, April 6, 2011, http://www.aviationweek.com/aw/generic/story_generic.jsp?channel=aerospacedaily&id=news/asd/2012/04/06/02.xml&headline=USAF%20Crafts%20New%20Light%20Air%20Support%20RFP.
[43] Interview with retired Air Force general officer, January 5, 2012.
[44] Ibid; Interview with Air Force major, February 16, 2012.
[45] Marcus Weisgerber, "Lawmakers Nix Light-Attack Aircraft Proposal," *Military Times*, October 14, 2011, http://www.militarytimes.com/news/2011/10/defense-lawmakers-nix-light-attack-aircraft-proposal-101411/. In 2011 the House Appropriations, House Armed Services, and Senate Armed Services committees rejected a $17 million request by U.S. Central Command (CENTCOM) for the Combat Dragon II program. In 2010 those same committees rejected a $22 million Department of Defense request to continue funding for the Navy-initiated Imminent Fury

program.; Robert F. Dorr, "Capitol Hill Rejects Light Attack Aircraft Request," Defense Media Network, October 21, 2011, http://www.defensemedianetwork.com/stories/capitol-hill-rejects-light-attack-aircraft-request. The Combat Dragon II program sought to identify a light-attack aircraft for COIN and counterterrorism missions in Afghanistan. CENTCOM argued that a turboprop such as the Super Tucano could provide effective support to ground troops at a dramatically lower cost than jet fighters. Similar to Combat Dragon II, the Imminent Fury program sought to test the effectiveness of light-attack turboprops in Afghanistan. The funding would have enabled the deployment of four leased Super Tucanos to Afghanistan for six months. The Kansas delegation, which favors the HBC AT-6 over the Embraer Super Tucano, pressured the committees to reject funding for Imminent Fury.

[46] "Remarks by Senator John McCain on the Conference Report of the FY2012 Omnibus Appropriations Bill," December 16, 2011, http://www.mccain.senate.gov/public/index.cfm?FuseAction=PressOffice.PressReleases&ContentRecord_id=48F0C068-A39A-0237-FB09-7FAF7546FB90. For example, when discussing his opposition to Combat Dragon II, Senator John McCain cited an uncompetitive bidding process for the aircraft selection and the lack of an urgent operational requirement. He also stated that the program was not requested by either the administration or the Pentagon.

[47] Interview with Richard Aboulafia, March 7, 2012.

[48] "Advanced Pilot Training (APT) Family of Systems (FoS) Program – Request for Information: Second Request," U.S. Air Force, August 5, 2009, https://www.fbo.gov/utils/view?id=f65874909e984d772cae27f9170b0346.

[49] Stephen Trimble, "US Air Force, Industry Prepare for T-38 Replacement," Flightglobal, June 22, 2010, http://www.flightglobal.com/news/articles/us-air-force-industry-prepare-for-t-38-replacement-343393/.

[50] Stephen Trimble, "USAF delays T-38 trainer replacement to 2020," Flightglobal, February 17, 2012, http://www.flightglobal.com/news/articles/usaf-delays-t-38-trainer-replacement-to-2020-368456/.

[51] "Advanced Pilot Training (APT) Family of Systems (FoS) Program," U.S. Air Force, Federal Business Opportunities, August 5, 2009, https://www.fbo.gov/index?s=opportunity&mode=form&tab=core&id=d493f09e6c5a91bf36509a4fbdccb3e8&_cview=0. The five desired training tasks for the T-X aircraft are sustained high-G operations, air-refueling, night vision imaging systems operations, air-to-air intercepts, and data-link operations.

[52] Stephen Trimble, "Lockheed Ponders T-50 Re-Engining for T-X Programme," Flightglobal, May 24, 2011, http://www.flightglobal.com/news/articles/lockheed-ponders-t-50-re-engining-for-t-x-programme-357148/.

[53] Amy Butler, "Alenia Proposing M-346 for U.S. Trainer," *Aviation Week*, September 24, 2009, http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/M346092409.xml&headline=Alenia%20Proposing%20M-346%20for%20U.S.%20Trainer. Alenia, an Italian company, is still considering whether or not to partner with a U.S. partner. Currently the M-346 has 52% U.S. content, but Alenia officials intend to increase that to over 60%.; Amy Butler, "Contractor Teams Shaping Up for T-X Work," *AviationWeek*, September 29, 2011, http://www.aviationweek.com/aw/generic/story.jsp?id=news/awst/2011/09/26/AW_09_26_2011_p34-373061.xml&channel=defense. Alenia is working on a light-attack kit concept that would allow the T-100 to be armed and serve in close air support roles during combat and then de-armed and returned to training. Partner candidates include Boeing, Raytheon, and L-3 Communications.

[54] Amy Butler, "T-X Mating Dance Continues With Industry and Congress," *Aviation Week*, September 21, 2011, http://www.aviationweek.com/aw/blogs/defense/index.jsp?plckController=Blog&plckBlogPage=BlogViewPost&newspaperUserId=27ec4a53-dcc8-42d0-bd3a-01329aef79a7&plckPostId=Blog%3A27ec4a53-dcc8-42d0-bd3a-01329aef79a7Post%3Ab5723c92-fe9a-41b5-b541-871fd660848a&plckScript=blogScript&plckElementId=blogDest.

[55] "L-3 Link Simulation & Training Joins BAE Systems Hawk AJTS Team to Pursue U.S. Air Force T-X Contract," BAE Systems, Inc., January 12, 2012, http://www.marketwatch.com/story/l-3-link-simulation-training-joins-bae-systems-hawk-ajts-team-to-pursue-us-air-force-t-x-contract-2012-01-12?reflink=MW_news_stmp.

[56] Butler, "Contract Teams Shaping Up." For the T-X competition, Lockheed Martin and KAI would take on more U.S. supplier content and find a domestic assembly location.

[57] Trimble, "USAF delays T-38 trainer replacement."

[58] Jay Menon, "BAE Wins New Trainer Order from India," *Aviation Week*, December 12, 2011, http://www.aviationweek.com/aw/generic/story.jsp?id=news/awx/2011/12/12/awx_12_12_2011_p0-405197.xml&channel=defense. The BAE Hawk T2 can be used as a ground attack or air defense aircraft and is capable of carrying rockets, bombs, and air-to-air missiles; "No. 76 Squadron," Royal Australian Air Force, http://www.airforce.gov.au/units/76sqn.aspx. They Royal Australian Air Force uses it BAE Hawk 127s both for

lead-in flight training and to provide close air support to Army operations; Greg Waldron, "PICTURES: KAI Rolls Out First Production T/A-50," *Flightglobal*, January 26, 2011, http://www.flightglobal.com/news/articles/pictures-kai-rolls-out-first-production-ta-50-352346/. In addition to serving as a lead-in fighter, the T/A-50 can carry air-to-air and air-to-surface weapons.

[59] SIPRI., "China."

[60] Flightglobal Insight, *World Air Forces 2011/2012*, http://www.flightglobal.com/airspace/media/reports_pdf/emptys/90190/world-air-forces-2011-2012.pdf; Jay Menon, "BAE Wins New Trainer Order from India," *Aviation Week*, December 12, 2011, http://www.aviationweek.com/aw/generic/story.jsp?id=news/awx/2011/12/12/awx_12_12_2011_p0-405197.xml&channel=defense.

[61] Bradley Perrett, "Indonesia Orders 16 T-50s From Korea Aerospace," *Aviation Week*, May 27, 2011, http://www.aviationweek.com/aw/generic/story_channel.jsp?channel=defense&id=news/asd/2011/05/27/05.xml; Florante S. Solmerin, "Spratlys Arms Race Heats Up; AFP to Buy Six Fighter Jets," *Manila Standard Today*, July 2, 2011, http://www.newsflash.org/2004/02/hl/hl110929.htm.

[62] Jung Sung-ki, "Source: Singapore Chooses Italy's M-346 Trainer Jet," DefenseNews, July 1, 2010, http://www.defensenews.com/article/20100701/DEFSECT04/7010310/Source-Singapore-chooses-Italy-s-M-346-Trainer-Jet; Siva Govindasamy, "UAE Stops Talks With Alenia Aermacchi on M-346 Contract," Flightglobal, February 24, 2011, http://www.flightglobal.com/news/articles/uae-stops-talks-with-alenia-aermacchi-on-m-346-contract-353563/. Alenia previously discussed a fighter variant of the M-346 with the United Arab Emirates.

[63] Interview with Air Force major, February 16, 2012.

[64] Interview with retired Air Force general officer, January 5, 2012.

[65] Interview with retired Air Force general officer, January 9, 2012.

[66] Interview with retired Air Force general officer, January 5, 2012.

[67] Flightglobal Insight, *World Air Forces 2011/2012*, 8, http://www.flightglobal.com/airspace/media/reports_pdf/emptys/90190/world-air-forces-2011-2012.pdf. "Active": Aircraft in day-to-day use; Stephen Trimble, "Egypt Named as F-16 Sales Candidate," Flightglobal, January 28, 2009, http://www.flightglobal.com/news/articles/egypt-named-as-f-16-sales-candidate-321733/.

[68] F-16.net, http://www.f-16.net/f-16_user.html. Only four of the 13 states that purchased the F-16 between 2000 and 2010 were acquiring it as a new airframe The four states acquiring the F-16 as a new airframe between 2000 and 2010 were Chile, Italy, Morocco, and Oman.

[69] Mark Thompson, "Sticker Shock: Iraqi F-16s $165 Million Each," *TIME* Battleland, September 28, 2011, http://battleland.blogs.time.com/2011/09/28/sticker-shock-iraqi-f-16s-165-million-each/#ixzz1ZFsmXwOf. The base price of the new F-16s being sold to Iraq is $165 million a plane; *SIPRI*, s.v. "Transfers." As a reference for used F-16 sales, in 2009 the Netherlands agreed to sell Chile 18 F-16C aircraft for $15 million each.; Siva Govindasamy, "Singapore Confirms Order for M-346 Trainer," Flightglobal, September 28, 2010, http://www.flightglobal.com/news/articles/singapore-confirms-order-for-m-346-trainer-347885/. Singapore recently ordered Alenia Aermacchi M-346s at a price of $28.3 million per aircraft.; "Hawk T2," RAF Valley, http://www.raf.mod.uk/rafvalley/aboutus/ajt.cfm. Currency calculation performed via Wolfram Alpha at http://www.wolframalpha.com/input/?i=convert+450+million+pounds+to+dollars+on+24+october+2006. The estimated cost for a BAE Hawk T2 is $30.1 million.; "Korea's T-50 Family Spreads Its Wings," Defense Industry Daily, January 5, 2012, http://www.defenseindustrydaily.com/koreas-t-50-spreads-its-wings-04004/. The estimated cost for a KAI T-50 is $20 million.

[70] The financial logic that has led to the fielding of advanced jet trainers by air forces in the developed world applies equally to states in the developing world. Advanced jet trainers, and their fighter variants, are cheaper to operate and maintain. Training the air crew also places less of a burden on government coffers. This economy of operation is one of the reasons air forces chose to operate the F-5 rather than buying used F-4 Phantoms, although the later was more capable.

[71] Richard Aboulafia, "Market Overviews: Trainer/Light Attack Aircraft," June 2011, Teal Group Corporation.

[72] Interview with Richard Aboulafia, March 7, 2012.

MAKING THE GRADE:
AN INTERNATIONAL REGULATORY FRAMEWORK FOR CYBERSECURITY

EMILY PEHRSSON

Vulnerable states, defined as states unable or unwilling to crack down on cyber crime within their borders, threaten U.S. cybersecurity. Current U.S. policy offers technology transfers to like-minded states to secure their cyber networks, without requiring these states to make cybersecurity a domestic policy priority. This brief proposes a voluntary, private-sector based cybersecurity grading system paired with security incentives administered through NATO to encourage improvements in cybersecurity. Participating states will be awarded grades based on the quality of their cybersecurity infrastructure. Incentives will increase incrementally with each security grade attained and include access to: (1) law enforcement training programs; (2) NATO cyber rapid reaction teams; (3) limited technology transfers; and (4) intelligence sharing. The proposed framework would initially apply to NATO members and would later be expanded to select non-member states. The grades framework and incentives will act as a short- to medium-term incentive for the rapid development of international cybersecurity standards and reduce long-term costs for the United States.

Strategic Importance of Cybersecurity

Increasing government, military, and industry reliance on the cyber domain has incentivized cyber crime and heightened the cost of internet disruptions. In 2010, cyber attacks rose 93% worldwide with approximately 55,000 pieces of malware introduced daily.[1] In 2011, U.S. authorities shut down a cyber botnet that stole $97 million and hijacked over 2 million computers, the majority of which were located in the United States.[2] The frequency and sophistication of cyber attacks will continue to rise as access to computers increases worldwide.[3]

Dangers of U.S. Cyber Insecurity

In 2010, the U.S. Computer Emergency Readiness Team (US-CERT) received 41,776 reports of malicious cyber incidents in federal networks, an increase of 39% since 2009.[4] Cyber attacks can threaten U.S. military operations, national critical infrastructure, information security, and economic competitiveness through:

- *Military Network Vulnerability*: From November 2008 to April 2009, the Pentagon spent approximately $100 million repairing damage from and addressing the

repercussions of cyber attacks.[5] Unauthorized users probe Department of Defense networks about 250,000 times every hour and over 6 million times per day.[6]

- *National Critical Infrastructure Vulnerability*: The U.S. Cyber Command only protects .mil domains, leaving the largely civilian-owned national critical infrastructure more vulnerable to attack. McAfee estimates that a major cyber crime attack would cost each company in the oil and gas sector approximately $8.4 million per day.[7] Deputy Defense Secretary William J. Lynn stated: "It is possible to imagine attacks on military networks or on critical infrastructure like the transportation system and energy sector that cause severe economic damage, physical destruction or even loss of life."[8]

- *Cost of Intellectual Property Theft*: McAfee estimates that intellectual property and proprietary information theft costs approximately $1 trillion annually.[9] The FBI stated that the cost to the United States equals about $400 billion every year.[10] Cyber criminals disproportionately target the United States. For example, Operation Shady RAT compromised the networks of over 71 organizations, two-thirds of which were in the United States.[11] A study released in 2010 by the Ponemon Institute estimated that each victim organization bears a median yearly cost between $1 million and $52 million as a result of cyber crime.[12]

Cyber Threats from Vulnerable States

Vulnerable states, such as Romania, Bulgaria, and Slovenia, are less willing and able to devote significant government resources to locating and extraditing cyber criminals and dismantling organized cyber crime groups, allowing these groups to threaten U.S. cybersecurity. A 2011 National Security Council report stated that "through cyber crime, transnational criminal organizations pose a significant threat to financial and trust systems…on which the world economy depends."[13] For example, through online fraud, cyber crime groups based in Central and Eastern Europe have cost U.S. citizens and organizations an estimated $1 billion annually.[14] Attacks by these groups have increased in frequency and number in the last five years.[15] Cyber criminals operating in vulnerable states threaten U.S. cybersecurity through:

- *Asymmetric Cyber Attacks*: Criminal organizations operating within these states are capable of threatening critical infrastructure, defense networks, and large corporations in the United States and globally. Because the technology needed for cyber weapons is cheap and easily accessible, criminal groups and hacktivists are able to conduct sophisticated and dangerous cyber operations.[16] For example, between 2007 and 2011, a cyber crime gang based in Estonia hijacked approximately four million computers in over 100 countries and stole approximately $14 million. U.S. businesses and government agencies, including NASA, and over 500,000 private citizens were among their targets.[17]

- *Connection to Drug Trafficking and Terrorism*: A July 2011 White House report stated that "virtually every transnational criminal organization and its enterprises are connected and enabled by information systems technologies, making cyber crime a substantially more important concern."[18] Terrorist groups use these illegal markets to finance operations.[19] For example, Al-Qaeda and Hezbollah actively recruit and train computer specialists or hire preexisting groups to facilitate their cyber operations.[20]

Barriers to Effective Cyber Domain Defense

Vulnerable states are less able to independently implement necessary cybersecurity standards because of the high cost of cyber defense and declining defense budgets.

- *Cost of Cyber Defense*: The cost of developing secure cyber networks can quickly overwhelm the budgets of vulnerable states. For instance, the Department of Homeland Security requested $233.6 million in order to deploy one cyber program, EINSTEIN 3, and coordinate threat notification among federal networks.[21] Over the next four years, the United States will allocate $10.5 billion annually to information security programs.[22]

- *Declining Defense Budgets*: Defense budgets are expected to decline as a result of austerity measures throughout Europe, including those of Bulgaria, Romania, Slovenia, the Czech Republic, Belgium, and Latvia. For example:

  - Slovenia cut its defense budget by 20% from 2010 to 2011 and plans to cut another 7% in 2012.[23]

  - Romania's defense budget is projected to decrease 30% between 2012 and 2015.[24]

Weaknesses of Current U.S. Cybersecurity Policy

U.S. policy now focuses on denial, awareness, and technology transfers to like-minded states. Elements of these approaches are valuable components of a comprehensive cybersecurity policy, but are insufficient to address the threat of cyber crime in vulnerable states.

Denial: Deterring Cyber Attacks through Passive Defense

DARPA, USCYBERCOM, and Pentagon officials plan to accelerate the development of technology for the defense of U.S. military and government networks through R&D programs. DARPA expects a 73% increase in cyber research funding in 2012, from $120 million to $208 million.[25] The White House appropriated $6 billion to strengthen its networks against cyber attack in 2008.[26]

- *Strength*: A significant investment in domestic cyber defense technology will decrease the probability of a successful cyber attack. Current initiatives include developing more Information Sharing and Analysis Centers (ISACs), which collect and disseminate real-time data to government networks and businesses.[27] This strategy will help network analysts to detect and respond to cyber attacks before they can infiltrate secure networks or damage infrastructure.

- *Weakness*: The hardware and software necessary to instigate a cyber attack is inexpensive and easily accessible. Malicious code is much simpler to write than defense software—for instance, some defense software requires 10 million lines of code, versus approximately 125 lines for malware.[28] The cost of repeated network intrusion or infection attempts is low, and new malware can be developed much more quickly than additional network defenses. Therefore, exclusively investing in denial capability in U.S. networks will not hamper the operation of foreign cyber crime groups and their ability to penetrate the best network defenses. Former Deputy Secretary of Defense William Lynn warned that "a fortress mentality will not work" and will leave U.S. networks vulnerable to determined criminal or hacktivist groups.[29]

Awareness Campaigns

The U.S. government is currently investing in cybersecurity awareness plans, especially for government employees, individuals working with national critical infrastructure, and financial sector employees.[30] These plans include programs designed to educate individual users on the importance of installing updates, safeguarding passwords, and following security protocols.

- *Strength*: 85% of the threat to U.S. cybersecurity networks can be eliminated with proper cyber hygiene, personal strategies by which individual users can improve their computers' security.[31]

- *Weakness*: While awareness can reduce basic network vulnerabilities, corporations, government employees operating with .gov domains, and ordinary citizens will not receive timely notification of cyber threats. Organized, determined hackers will still be able to penetrate many networks' security software.

Guaranteed Technology Transfers to Like-Minded States

Recognizing the cyber threat from vulnerable states, the White House proposed unconditional capacity building for U.S. allies to improve network interoperability, response time, and resilience. This plan includes limited technology transfers, information exchange, and clarifying standard operating procedures between states.[32] Similarly, the Cybersecurity Act of 2012 (S. 2105) proposes prioritizing foreign aid to states planning to allocate that aid for cybersecurity development.[33]

- *Strength*: U.S. allies will be significantly better equipped to confront emerging cyber challenges. Response times to attacks will decrease as a result of regular cooperation between allies and interoperable network systems.

- *Weakness*: Offering unconditional technology transfers and network assistance does not encourage our allies to make cybersecurity a budgetary priority. Global austerity measures threaten governments' defense budgets, and states that know they can rely on U.S. technology transfers will likely not invest as much in domestic R&D, cyber specialist training, or policy reform. A policy of guaranteed technology transfer will reduce global innovation and result in a larger budgetary burden for the United States. Similarly, the Cybersecurity Act of 2012 does not require states to make their own advancements in order to receive aid. Instead, they must simply express their intention to use the money for cyber capacity building.[34] Furthermore, hackers and organized criminal groups from any state can threaten U.S. networks. Therefore, cooperating with only the closest U.S. allies leaves networks open to a range of threats from other states.

Components of these policies are necessary for a successful comprehensive cybersecurity strategy. However, they fail to account for declining defense budgets and the lack of independent cyber innovation programs among vulnerable states. An international framework that encourages states to rapidly upgrade their cybersecurity capability and law enforcement is a critical step in securing U.S. networks against cyber crime.

International Cyber Grade Framework

To encourage vulnerable states to make cybersecurity a priority, this brief proposes the creation of an international Cyber Grade Framework (CGF) paired with security incentives.

Targeted States

The primary purpose of this policy is to facilitate the implementation of rigorous cybersecurity standards in order to hinder the operation of cyber crime and hacktivist groups. It targets vulnerable states that desire to reduce cyber crime within their borders but are unwilling or unable to earmark sufficient government funds to do so. The CGF should apply primarily to vulnerable states, particularly those with a GDP of at least $10 billion. States that meet this budgetary guideline should have the capability to implement functional cybersecurity standards with the assistance of the international community.

- *Initial Region – Eastern Europe*: The initial stage of the policy will primarily target Eastern European NATO-member states. Eastern Europe is a known base for numerous cyber crime groups, which frequently target the U.S. financial sector.[35] In the past, the United States and NATO have successfully cooperated with Eastern European states primarily on short-term law enforcement operations to combat cyber

crime. This collaboration establishes a promising precedent for more substantial long-term cooperation.

- *Future Policy Expansion – Central Asia, Africa and the Middle East*: Once the CGF has been tested with NATO members, it will be expanded to target regions outside of Eastern Europe, namely Central Asia, Africa, and the Middle East. Combating illegal cyber activity in these regions will significantly hinder the ability of money launderers, drug traffickers, and terrorists to operate.[36] NATO/U.S. relations with these states are more sensitive than in Eastern Europe, but previous successful cooperation indicates the potential for a constructive relationship to combat transnational cyber crime.[37]

- *Exclusion of Russia and China*: Russia and China, which are suspected of cooperating with transnational groups to launch cyber attacks, would not be invited to participate in the proposed framework. This policy aims to assist vulnerable states that wish to cooperate closely with NATO and the United States and contribute to a more secure international cyber domain.

Baseline Assistance

States that do not participate in the CGF remain a threat to U.S. national security. To address this threat, NATO will:

- *Provide a Complementary Network Vulnerability Assessment*: A team of independent cyber analysts will complete a complementary assessment of the state's network vulnerability and the cost of intellectual property theft to the national economy.

- *Allow Limited Access to Cybersecurity Conferences*: NATO may also allow limited access to CGF cybersecurity conferences in order to encourage the state to opt into the voluntary international regulations.

- *Emphasize Compliance with Cybersecurity Norms*: Through diplomatic channels, the United States will emphasize that "cyber crime originating in or occurring within their jurisdiction is a serious crime with international implications," and they need to develop their legal systems to prosecute these crimes.[38]

Private Sector Framework

The CGF is based on a private-sector incentive model designed to encourage companies to implement cybersecurity standards without government mandates.[39] This model is the best approach to encourage higher cybersecurity standards in the absence of compulsory international cybersecurity standards. States will voluntarily adopt a grade's requirements in order to receive the associated incentives, encouraging them to make cybersecurity a

priority. Simultaneously, this policy will strengthen participating states' ties with the international community, creating a more secure global network.

Grade One: The purpose of this grade is to foster cyber technology innovation to encourage rapid progress towards secure networks.

Requirements

- Increase cybersecurity R&D budget by 10% from the amount allocated in the year of accession to the CGF.

    - For a period of five years after achieving Grade 1, the state must keep the cyber R&D budget at the required level, correcting for inflation.

    - Through increased R&D budget allocations, states will be capable of promoting independent domestic innovation. Additionally, they have the option of cooperating with existing research programs at the Cooperative Cyber Defence Center of Excellence (CCDCoE) in Estonia.[40]

Incentives

- Allow admittance to CGF international cybersecurity conferences.

- Implement cyber law enforcement training programs and provide international teams to assist in capacity building for law enforcement personnel.

Grade Two: The purpose of this grade is to facilitate intelligence sharing and install basic law enforcement/extradition standards to allow international cybersecurity cooperation.

Requirements

- Ensure compliance with CGF's security breach notification regulations.

    - CGF members are required to disclose information regarding criminal organizations that may threaten other member states in the CGF information clearinghouse, a new international body that will facilitate the exchange of information between states (see below).[41]

    - Members must implement a domestic framework within the government, to which corporations and individuals can report network breaches and cyber attacks.

- Implement minimum extradition guidelines.

- Extradition standards are governed by Article 24 of the Budapest Convention on Cybercrime. States meet the standard by ratifying the treaty and adhering to its cybercriminal extradition guidelines.[42]

- Officials appointed under the G-8 24/7 Cyber Crime Network will act as points of contact for intelligence exchange and extradition issues.[43] States that have not established a designated official will be required to do so.

Incentives

- Provide rapid reaction cyber teams following a cyber incident involving critical infrastructure to rebuild network defenses and improve resiliency.[44]

- Facilitate intelligence sharing between member states.

  - CGF will establish a clearinghouse for information on emerging cyber threats. Pertinent threat information will be transferred to states achieving Grade 2.

  - If information pertaining to a lower-grade state is received, the information may be shared at the discretion of the CGF clearinghouse and with the permission of the informing state.

- Supply limited technology transfers.

  - Technology transfers from the United States associated with this framework will be governed by the Department of Defense Technology Disclosure Policy.[45]

Grade Three: The purpose of this grade is to facilitate high-level cooperation between cyber law enforcement teams and military units to increase network resiliency and reduce incident response time.

Requirements

- Create a cybersecurity branch of law enforcement that is compliant with CGF standards. To achieve compliance, member states must have:

  - A national Computer Emergency Readiness Team, which can manage several domestic cyber threat databases and work with international teams in attribution operations;

  - A public notification system to inform non-government organizations of emerging cyber threats;

  - A database and notification system for authorized government employees to defend government networks and improve response time to cyber threats.[46]

- Engage in joint training of personnel with Grade 3 states in order to increase the efficiency of inter-state operations and communication. Re-training for international network coordination personnel must occur every three years.

Incentives

- Participate in joint military operations with the United States and other Grade 3 states. Exercises will focus on solidifying protocols for incident response and lessening the time necessary to restore network functionality following a variety of attacks.

- Expanded access to NATO rapid reaction cyber teams for a wider range of threats, including the cases of a denial of service cyber incident or information theft from government networks.

CGF Oversight and Compliance

NATO will administer the cybersecurity private-sector framework through a compliance organization modeled after the IAEA. This model was selected because of its applicability to a sensitive industry critical to national security. The organization will ensure compliance with enumerated standards.

- *Structure*: Within NATO, the CGF will be semi-autonomous, but it will report to NATO's North Atlantic Council. It will also act as a clearinghouse for cybersecurity information and coordinate with NATO's Cooperative Cyber Defence Centre of Excellence in Estonia for research and development.[47]

- *Main Administrative Bodies*: Two primary administrative bodies will design and execute policy for the organization:

    1) *General Conference*: The General Conference is composed of CGF member states. Once a state opts into the first cybersecurity grade, it receives one vote in the General Conference. This body will meet annually to approve measures recommended by the Board of Governors. Additionally, it will perform bi-annual audits of member states' security standards and report the findings to the Board of Governors for review. States may request that teams inspecting its facilities be accompanied by state representatives.

    2) *Board of Governors*: The Board of Governors will be composed of NATO Grade 3 states only. It will present policy and budget recommendations to the General Conference. It will be responsible for state suspensions and statute amendments and will meet five times per year to guide the General Conference.[48]

- *Member Accession Process*: States intending to join the oversight organization must meet the following requirements:

1) Applicant state achieves one of the three cybersecurity grades as defined by the aforementioned regulations and verified by the General Conference.

2) NATO's North Atlantic Council approves the application with a 2/3 majority.

3) General Conference approves the application with a 2/3 majority.

- *Cost of Membership*: States will be required to pay low dues for membership in the CGF in order to cover approximately one-half of the organization's costs. NATO will pay the remaining costs, which will be significantly less expensive than the cost of the free technology transfers, rapid reaction teams, and legal training currently in place.

Strengths of the Proposed Cybersecurity Framework Policy

The CGF uses incentives to foster greater cybersecurity capability and provides the following benefits:

- *Cost Effectiveness*: Rather than providing free technology transfer to numerous states in order to update their cybersecurity systems, this policy requires states to make cybersecurity a domestic budget priority. Many of the costs of research and installation will be borne by participating states, while NATO will provide the expertise necessary to ensure the most effective practices and infrastructure are used.

- *Promotes International Innovation*: States will invest in their own R&D projects, prompting global innovation. The United States and other key cyber powers will not be alone in developing new technologies and methods, allowing for a more versatile, resilient global cybersecurity network.

- *Solidifies International Cybersecurity Norms*: Currently international cybersecurity norms regarding cyber criminals and hacktivists are absent or vague. Implementing this framework will clarify and bolster these norms, allowing NATO to hold states to an international standard and encourage more international cooperation on issues pertaining to cyber crime.

- *Increases Network Communication Speed*: In order to reach the highest cybersecurity grade, states must participate in joint training to facilitate intelligence sharing, early warning systems, and joint cyber operations. Joint personnel training will decrease response time and increase resilience of all member states' networks.

Possible Objections to the Proposal

- *Objection*: States will not to opt into the CGF because they fear U.S. interference in their networks.

  Response: The two-stage policy is designed to reassure non-NATO members that the CGF can be implemented without U.S. interference in sensitive network technology. Additionally, Eastern European states have successfully cooperated with the United States and NATO, yielding positive results.

  - *Estonia*: Following the 2007 Denial of Service attacks, which disrupted the Estonian financial sector networks, Estonia invited the United States to assist with damage control and rehabilitation of the networks. Since 2007, Estonia and the United States have worked with NATO to establish the Cooperative Cyber Defense Centre of Excellence (CCD COE) to promote cyber technology R&D.

  - *Slovenia*: From 2007 to 2011, the FBI worked with the Slovenian Cyber Emergency Readiness Team (SI-CERT) to take down an international botnet, which threatened the networks of several countries. The criminals operating the botnet were identified and convicted because of cooperation between the two agencies.[49]

- *Objection*: The United States will not allow CGF teams to inspect its cybersecurity structures to ensure compliance with CGF regulations.

  Response: International compliance teams have been used previously in highly sensitive military sectors, such as nuclear weaponry. For example, in 1967 the United States agreed to "permit the International Atomic Energy Agency to apply its safeguards to all nuclear activities in the United States–excluding only those with direct national security significance."[50] Inspection teams will always be accompanied by representatives of the member state if requested.[51] Furthermore, the CGF inspection teams will not need access to sensitive cyber technology. Rather, teams will perform detailed inspections of law enforcement agencies, general budgets, and extradition records.

- *Objection*: The United States and NATO will be reluctant to provide technology transfers to states developing cyber capabilities.

  Response: Current U.S. and NATO policies provide technology transfers to states developing their cybersecurity capabilities. This proposal differs from precedent only in that the United States and NATO will not be providing technology transfers freely but rather as an incentive to reward compliance with the voluntary regulations. Currently, NATO-verified Centers of Excellence develop and transfer technology to member states. Additionally, the DoD Defense Technology Security Administration approves approximately 30,000 export licenses annually for controlled hardware and technology.[52]

Conclusion

Cybersecurity is vital to preserving stability in the financial sector, military readiness, and critical infrastructure. States must rapidly advance their cybersecurity capabilities to keep pace with growing challenges. Most states are currently at dramatically different levels of cyber capability, impeding their ability to communicate and participate in joint operations.

The CGF will encourage states to prioritize cybersecurity in their budgets and meet voluntary regulations to receive security incentives. This proposal will foster innovation and facilitate the transition to a higher level of cybersecurity, cooperation, and law enforcement capability. The advancements from the CGF will create more secure global networks, capable of confronting a critical 21st century threat.

---

[1] "Symantec Report Finds Cyber Threats Skyrocket in Volume and Sophistication," *Symantec Corporation*, April 5, 2011, http://www.symantec.com/about/news/release/article.jsp?prid=20110404_03.; Michael Cooney, "US cyber chief says cloud computing can manage serious cyber threats," *Network World*, November 7, 2011, http://www.networkworld.com/news/2011/110711-cyberchief-cyberthreats-252844.html?hpg1=bn.

[2] A botnet is a "computer robot," which is created when a user intentionally or unintentionally downloads malware to his computer. A "botherder" or "botmaster" is then able to control that computer from his base computer. Botnets can contain hundreds of thousands of computers, which are then capable of instigating denial-of-service attacks, for example. "Bots and Botnets—A Growing Threat," *Norton Antivirus*, accessed January 20, 2012, http://us.norton.com/theme.jsp?themeid=botnet; Dean Wilson, "US Shuts Down a Major Cyber Crime Botnet," *The Inquirer*, April 14, 2011, http://www.theinquirer.net/inquirer/news/2043439/shuts-major-cyber-theft-botnet.

[3] *Cybersecurity: Responding to the Threat of Cyber Crime on Terrorism*, *Testimony before the Senate Judiciary Committee Subcommittee on Crime and Terrorism*, 112th Congress (April 2011) (Statement of Gordon M. Snow, Assistant Director, Cyber Division, FBI), http://www.fbi.gov/news/testimony/cybersecurity-responding-to-the-threat-of-cyber-crime-and-terrorism.

[4] Elizabeth Montalbano, "Federal Cyber Attacks Rose 39% In 2010," *InformationWeek*, March 23, 2011, http://www.informationweek.com/news/government/security/229400156.

[5] Lolita C. Baldor, "Pentagon spends $100 million on cyber attacks," *MSNBC Security*, April 7, 2009, http://www.msnbc.msn.com/id/30090749/ns/technology_and_science-security/t/pentagon-spends-million-cyber-attacks/#.T1ZL5_XksW1.

[6] "CSIS Cybersecurity Policy Debate Series: U.S. Cybersecurity Policy and the Role of U.S. CYBERCOM," *Center for Strategic and International Studies*, June 3, 2010, http://csis.org/files/attachments/100603csis-alexander.pdf, 5.

[7] Stewart Baker et al., "In the Crossfire: Critical Infrastructure in the Age of Cyber War," *McAfee, Inc.*, 2009, http://www.mcafee.com/us/resources/reports/rp-in-crossfire-critical-infrastructure-cyber-war.pdf, 10.

[8] U.S. Department of Defense, John D. Banusiewicz, "Lynn Outlines New Cybersecurity Effort," June 16, 2011, http://www.defense.gov/news/newsarticle.aspx?id=64349.

[9] Matthew Hansen, "U.S. on Offense in Cyberwar?" *Omaha World-Herald*, November 20, 2011, www.omaha.com/article/20111120/NEWS01/711209927.

[10] Gordon M. Snow, *Cybersecurity: Responding to the Threat of Cyber Crime on Terrorism*.

[11] Operation Shady RAT (Remote Access Tool) was an ongoing cyber attack initiated in 2006 and reported in 2011 by McAfee. The Republic of China is widely accepted as the likely perpetrator. A large number of the victim companies and organizations did not realize their networks had been compromised. Dmitri Alperovitch, "Revealed: Operation Shady RAT," *McAfee Inc.*, March 6, 2012, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf.

[12] Gordon M. Snow, *Cybersecurity: Responding to the Threat of Cyber Crime on Terrorism*.

[13] Kathleen Hickey, "How International Cyber Crime Threatens National Security," *Government Computer News*, July 27, 2011, http://gcn.com/articles/2011/07/27/international-cyber-crime-threat-to-us.aspx.

[14] U.S. White House, "Strategy to Combat Transnational Organized Crime," Accessed March 6, 2012, http://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf, 7.
[15] Gerry Smith, "Cyber-Crimes Pose 'Existential' Threat, FBI Warns," *Huffington Post*, January 12, 2012, http://www.huffingtonpost.com/2012/01/12/cyber-threats_n_1202026.html.
[16] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace," July 2011, http://www.defense.gov/news/d20110714cyber.pdf, 3.
[17] "US Shuts Down Cyber Crime Gang," *Irish Times*, November 10, 2011, http://www.irishtimes.com/newspaper/breaking/2011/1110/breaking53.html.
[18] U.S. White House, "Strategy to Combat Transnational Organized Crime."
[19] Clay Wilson, *Botnets, Cyber Crime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress,* CRS Report for Congress (The Library of Congress: Congressional Research Service, January 29, 2008), http://www.fas.org/sgp/crs/terror/RL32114.pdf, 2, 30.
[20] Raphael F. Perl, *Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation* (Organization for Security and Cooperation in Europe, April 7, 2008), http://www.osce.org/atu/31428.; "Cyber Security and Terrorism," *Interfor*, March 6, 2012, http://www.interforinc.com/FileLib%5CCyberterrorism.pdf, 3.
[21] U.S. Department of Homeland Security, "FY 2012 Budget in Brief," Retrieved January 12, 2012, http://www.dhs.gov/xlibrary/assets/budget-bib-fy2012.pdf, 11.
[22] "Cyber Security and Terrorism."
[23] "Defence Budget (Slovenia) - Sentinel Security Assessment - The Balkans," *Jane's Information Group*, December 26, 2011, http://articles.janes.com/extracts/extract/balksu/slovs090.html.
[24] "Research and Markets: The Romanian Defense Industry – Market Opportunities and Entry Strategies Analyses and Forecasts to 2015," *Business Wire*, December 27, 2011, http://www.businesswire.com/news/home/20110506005294/en/Research-Markets-Romanian-Defense-Industry---Market.
[25] Jim Wolf, "U.S. Says Will Boost Its Cyber Arsenal," *Reuters*, November 7, 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107.
[26] Bobbie Johnson, "NATO says cyber warfare poses as great a threat as a missile attack," *The Guardian*, March 5, 2008, http://www.guardian.co.uk/technology/2008/mar/06/hitechcrime.uksecurity.
[27] U.S. Department of Homeland Security, "Blueprint for a Secure Cyber Future," November 2011, http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/blueprint-for-a-secure-cyber-future.pdf, 7.
[28] Jim Wolf, "U.S. Says Will Boost Its Cyber Arsenal," *Reuters*, November 7, 2011, http://www.reuters.com/article/2011/11/07/us-cyber-usa-offensive-idUSTRE7A640520111107.
[29] William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010).
[30] U.S. Department of Defense, "Department of Defense Strategy for Operating in Cyberspace."
[31] U.S. House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force," October 2011, http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf, 12.
[32] U.S. White House, "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World," May 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, 19.
[33] Cybersecurity Act of 2012, S. 2105, 112th Cong. (2012) http://www.hsgac.senate.gov/imo/media/doc/CYBER%20The%20Cybersecurity%20Act%20of%202012%20final.pdf.
[34] Ibid.
[35] Clay Wilson, *Botnets, Cyber Crime, and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress*.
[36] Ibid.
[37] For example, the 2004 Istanbul Cooperation Initiative (ICI) established bilateral military cooperation between NATO and states in the Middle East. Members include Bahrain, Qatar, Kuwait, and the UAE. The initiative promotes military interoperability, intelligence sharing, and participation in NATO exercises. Additionally, in February 2012, the U.S. Air Force and Kyrgyzstani Ministry of Defense exchanged intelligence on sensitive systems and tactics, including chemical weapons and CBRNE procedures. This cooperation continued a precedent of intelligence sharing between the United States and Kyrgyzstan. Istanbul Cooperation Initiative (ICI), November 18, 2011, http://www.nato.int/cps/en/SID-52237F1C-F7242949/natolive/topics_58787.htm?; Lynsie Nichols, "US,

Kyrgyz share EOD, CBRNE Techniques," February 27, 2012, http://www.manas.afcent.af.mil/news/story.asp?id=123291439.
[38] U.S. House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force," October 2011, http://thornberry.house.gov/UploadedFiles/CSTF_Final_Recommendations.pdf, 18.
[39] U.S. House of Representatives, "Recommendations of the House Republican Cybersecurity Task Force."
[40] CCDCoE was founded in 2008 and promotes the development of cyber technology. Based in Tallinn, Estonia, it is sponsored by several states including Estonia, the United States, Latvia, Lithuania, Germany, Italy, and Poland. NATO, and Active Command Transformation specifically, uses this facility to develop new cyber technology and policy. NATO Cooperative Cyber Defense Center of Excellence, http://www.ccdcoe.org/.
[41] See "CGF Oversight and Compliance" section for additional information.
[42] Convention on Cybercrime, November 23, 2001, UNTC I-40916.
[43] Raphael F. Perl, "Terrorist Use of the Internet: Threat, Issues, and Options for International Co-operation."
[44] National Critical Infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Critical Infrastructures Protection Act of 2001, §5195 (2001).
[45] The National Disclosure Policy provides guidelines for the disclosure of classified military information (CMI) to foreign governments and/or organizations. U.S. Department of Defense, "National Disclosure Policy: Chapter 3 – Technology Transfer and Disclosure," October 3, 2003, http://www.dsca.mil/samm/Chapter%2003%20-%20Technology%20Transfer%20and%20Disclosure.pdf.
[46] See the U.S. Federal Vulnerability Knowledgebase. U.S. Computer Emergency Readiness Team, "Analytical Tools and Programs: Government Users," February 24, 2012, http://www.us-cert.gov/federal/analytical.html.
[47] "NATO and Cyberdefence," September 16, 2011, http://www.nato.int/cps/en/SID-63B85F2D-2CA198C8/natolive/topics_78170.htm?.
[48] Suspensions can occur when a state initially implements the guidelines necessary for a grade, but it fails to maintain the provision requirements. They may also occur if a state grossly endangers the security of CGF members' networks via cooperation with transnational crime groups or otherwise. The board of governors has the option of demoting the state's grade or suspending it from the CGF.
[49] Slovenian Computer Emergency Readiness Team (SI-CERT), "SI-CERT Prejel Priznanje FBI," January 17, 2012, http://www.cert.si/.
[50] Agreement between the United States of America and the International Atomic Energy Agency for the Application of Safeguards in the United States (and Protocol Thereto), November 18, 1977, TIAS 6839, http://www.state.gov/t/isn/5209.htm.
[51] Ibid.
[52] U.S. Department of Defense, "Defense Technology Security Administration," http://www.dtsa.mil/.

CROWDSOURCING GLOBAL SECURITY:
FIGHTING PANDEMIC DISEASE IN THE INFORMATION AGE

EFRAT ROSENZWEIG

Pandemic disease constitutes a threat for which we are nationally and globally unprepared. Left unchecked, pandemic disease can lead to millions of deaths, shifts in the balance of power, resource wars, mass migration, and state failure.[1] The ability to prevent pandemics hinges on early detection. Epidemiological surveillance in areas where novel viruses are likely to emerge, however, is rudimentary, allowing most diseases to spread undetected.[2] Reliance on inadequate reporting is a dangerous oversight that potentially compromises national and global stability.

This brief proposes an alternative method of preventative surveillance that uses crowdsourcing technology to provide states with real-time data on potential epidemiological threats. Based on reporting by health professionals, this system will create a map on which clusters of similar cases indicating a possible epidemic could be observed. Ultimately, information sharing between states in the field of public health will provide a basis for increased cooperation to combat other transnational security threats, including organized crime and terror.

Dangers of Pandemic Disease

Between 50 and 100 million people were killed by the Spanish influenza epidemic of 1918, a virus believed to be a strain of avian flu.[3] Other viruses, like the measles and polio, are more infectious than influenza and could be more fatal.[4] While high casualties alone are a threat to human security, pandemics affect traditional security issues as well.

- Pandemics can precipitate violent conflicts and determine their outcome.[5] A state affected by an epidemic may experience a decline in military capability, resulting in destabilizing shifts in regional balances of power.
    - For example, the Spanish flu of 1918 emerged in Austria-Hungary in 1917, a year before it reached Allied troops. Mortality rates were highest in Germany and

Austria-Hungary and lowest in England and France. In particular, the pandemic dramatically reduced the number of troops available for the German offensive in the spring of 1918 which could have led to a victory for the Central Powers.[6] The difference in mortality contributed to the Allied victory in World War I.[7]

- States that lose the capacity to provide vital services to their citizens are more vulnerable to criminal and insurgent groups. Further, as an epidemic spreads, governments will be crippled by widespread police and military absenteeism.[8] As a result of this decreased capacity, states will be more likely to collapse.

- Epidemic disease can lead to a significant disruption of the adult workforce and damage international trade, causing an economic decline and contributing to domestic instability. States with high disease burdens are more prone to insurgencies and high crime rates.[9]

    - HIV/AIDS is expected to cause a 60% decline in South Africa's GDP by 2050.[10] The beginnings of this economic decline have contributed to riots in many of the poverty-stricken townships surrounding South Africa's cities and boycotting of elections in areas where the ANC enjoyed strong support before the AIDS pandemic began.[11]

- Vaccine development for a novel pathogen can take anywhere from two months to twenty years.[12] During an epidemic, countries with vaccine manufacturing capability would give priority to their own populations.[13] The supply of vaccines available to developing countries will be limited due to stockpiling by high income countries.[14] This will increase tensions between developing and developed countries and may also lead to interstate conflict as states compete for limited medical resources.

    - When H5N1 Avian flu emerged in Indonesia in 2005, Tamiflu was unavailable to Indonesian buyers, as the drug had been stockpiled by wealthy countries. Samples of the virus were sent by Indonesia to the WHO and then to an Australian pharmaceutical company for vaccine development. The manufacturer did not intend to sell a potential vaccine in Indonesia.[15] In February 2007, the Indonesian Health Ministry announced that they would cease virus sharing for testing and drug development unless new terms were negotiated by the WHO that would be more beneficial to developing countries.[16]

- Pandemics increase the probability of refugee crises as people flee affected countries, contributing to food and water shortages and exacerbating regional tensions.[17] If the crisis persists, mass migration can cause intrastate conflict.[18]

- Since 2008, over three million people have fled Zimbabwe to South Africa. In addition to the political instability in Zimbabwe, many are fleeing cholera and the AIDS epidemics; others are disease victims seeking treatment that is unavailable in Zimbabwe's collapsed health system. South Africa has labeled refugees as "voluntary economic migrants," which denies them legal status and government protection. Tensions have steadily increased as the refugee population has grown and, in May 2008, these tensions erupted in violence against the refugees that killed 60 and further displaced over 25,000.[19]

International security analysts have traditionally categorized pandemic disease as a global health or humanitarian issue.[20] Since the SARS and H1N1 scares and with the threat of avian flu looming, it has become increasingly clear that pandemic disease has real security implications that cannot be ignored. As with any threat, the first line of defense is accurate intelligence.

Status of Epidemiological Surveillance

While most developed countries have highly effective epidemiological surveillance systems, the majority of developing countries do not.[21] This lack of surveillance is dangerous, as agrarian communities without proper sanitation provide an ideal breeding ground for novel viruses.[22]

Surveillance in the U.S.: A Problematic Model for Developing Countries

The U.S. uses a population-based model, in which doctors record diseases classified by the World Health Organization as "reportable," such as cholera and H5N1 influenza.[23] The U.S. Centers for Disease Control and Prevention (CDC) responds to these reports through several programs:

- The Office of Surveillance, Epidemiology, and Laboratory Services (OSELS) examines birth, death, and medical records in order to compile statistics on the frequency of reportable diseases.[24]

- The National Center for Emerging and Zoonotic Infectious Diseases (NCEZID) coordinates the government's response to outbreaks.[25]

- The Office of Public Health Preparedness and Response (PHPR) monitors reporting systems and maintains the strategic national stockpile of medical supplies.[26]

Most developing countries use the U.S. method as a model for their own surveillance systems. Among these countries, low reporting rates and inadequate data analysis are pervasive.[27] This is primarily because:

- Low income countries have a severe shortage of health professionals, most of whom have neither the time nor the inclination to complete the requisite paperwork.[28]

- The U.S. spends close to $2 billion per year on infectious disease prevention.[29] Low income countries cannot afford such a costly surveillance system.

Surveillance in Developing Countries

Most developing countries have modified the U.S. model in an attempt to decrease costs. These adaptations make surveillance systems less effective and are inadequate.

- Due to the cost of a population-based model, most countries use sampling, which gathers information on only 10-20% of patients.[30] The vast majority of patients and illnesses go unreported.

- Sentinel sites–major hospitals with staff willing to report regularly–conduct sampling.[31] In many developing countries, only the wealthy can afford to seek care at these hospitals.[32] Low-income patients, who are most likely to be infected with zoonotic- or animal borne- diseases, do not have access to these sites.

- Most states have no enforcement mechanism to ensure reporting. The forms are lengthy and compliance is low.[33] The average reporting rate in developing countries is 7-8%.[34]

These factors produce a highly inefficient system that can allow pathogens to spread unchecked through a population and across borders.

Current Initiatives to Improve Global Epidemiological Surveillance

Humanitarian projects to improve reporting fit broadly into two categories: those that seek to improve the ability of developing nations to conduct their own epidemiological surveillance and those that seek to bypass governments and gather information independently.

Capacity-Building Programs

Programs to improve the ability of developing countries to obtain accurate statistics on infectious diseases are appealing because they are, theoretically, a one-time cost with continuing returns. The most significant of these programs are:

- The CDC's Global Disease Detection Program, which aims to establish 16 centers worldwide that will serve as laboratory and information-gathering systems on global infectious diseases.

  Weakness: Only six of these centers have been built due to budget shortages.[35] Those that exist only analyze samples of reportable diseases. Many doctors are reluctant to cooperate with CDC labs due their affiliation with the United States.

- The Field Epidemiology Training Program (FETP), which seeks to train local epidemiologists in the developing world.[36]

  Weakness: The primary job of FETP graduates is to trace outbreaks back to patient zero after they occur. This has little preventative value.

- WHO-Afro's Integrated Disease Surveillance and Response Program, which assesses surveillance systems and recommends improvements.

  Weakness: Only 4 of 46 participating countries have undergone analysis, as the WHO does not fund improvements to existing systems.[37]

These issues weaken the ability of capacity-building programs to improve surveillance. Most programs never reach the rural agrarian communities that are most at risk for emerging diseases.

Independent Monitoring Programs

Rather than improving government capacity to reach poverty-stricken rural populations, some organizations have developed programs to gather information independently of governments. These include:

- WHO's Program for Monitoring Emerging Diseases (ProMED), which reports on outbreaks of zoonotic diseases in member states [38] Information comes from

government reports and independent sources, including media reports, local observers, and online sources.[39]

Weakness: While it does include non-government sources, ProMED still relies on secondary information, rather than direct reporting by health professionals.

- The Peruvian Navy's AlertaDISAMAR, which is a local effort to use crowdsourcing technology to improve reporting from naval hospitals. The internet-based system allows doctors to use cell phones to submit information on reportable diseases.[40]

  Weakness: Limited resources and lack of cooperation from other segments of government have resulted in the system being limited to naval hospitals. Population-wide surveillance is not possible.

While government programs do not make full use of innovations in information technology, independent programs generally take advantage of the internet to gather large quantities of information quickly. This coincides with a general trend in the global health community of using information technology to improve health in the developing world. Existing projects, however, have failed to significantly improve surveillance. New technologies are now available that will make it possible to gather accurate, real-time data on diseases.

The Promise of Crowdsourcing

The newest innovation in information-gathering technology is crowdsourcing.[41] Users can post to an application with any internet-capable device, and their post appears as a pinpoint on a map.

The first application of crowdsourcing to disease monitoring came in 2010 with OutbreakMD, a smart phone application that uses this technology to allow doctors to post information on reportable diseases to HealthMap.[42] Using crowdsourcing for disease monitoring is a vital innovation that will provide the basis for new epidemiological surveillance systems.

OutbreakMD: Crowdsourcing in Global Health

During a pilot program in Port-au-Prince, Haiti, the program was embraced by the general public but generated a very low reporting rate amongst health professionals: only 117 reports were made by doctors over three months.[43] HealthMap itself receives no reports from most of Africa, Asia, and South America.[44] The low reporting rate can be attributed to a number of weaknesses in the program:

- Any person with internet access can post to OutbreakMD, which generates too much "noise", or inaccurate data, and is easily tampered with. OutbreakMD is a traditional crowdsourcing application; it is based on the premise that a large number of reports from all people with internet access will generate patterns faster than expert reporting. However, disease diagnosis requires medical training, and amateur diagnoses are typically incorrect.[45]

- The form is only available in English and has no place to enter patient age range, gender, or ethnicity.[46]

- The form relies entirely on the GPS function. It does not have a field for patient address, and the application is not programmed to extrapolate map data from that address. In many developing countries, patients travel large distances to seek care, meaning that a disease is not always located in the place where it is reported.[47]

- The lack of built-in analysis puts a heavy burden on health provision services.

- HealthMap does not send region-specific reports to health professionals automatically. Doctors must access HealthMap to see the map. Given the shortage of doctors in most developing countries, many do not have time to check HealthMap regularly.[48]

- Information is made public through HealthMap, limiting the willingness of countries to allow their doctors to participate.[49] Governments are reluctant to publicize potential internal weaknesses.

If the issues listed above were remedied, OutbreakMD would be a useful tool for providing vital statistics on endemic, reportable diseases to local governments. It would not, however, be useful for tracking emerging pathogens or potential pandemics because:

- The OutbreakMD form can only be submitted on reportable diseases, as defined by the WHO.[50] This limits its effectiveness in detecting emerging diseases.

- The raw data obtained by OutbreakMD are not analyzed for patterns associated with epidemics.

While OutbreakMD represents the most promising innovation in epidemiological surveillance, there is room for significant improvement. In order to be useful for pandemic prevention, a similar application must be able to cope with the volume of incoming data and,

more importantly, it must overcome the political and economic issues preventing health professionals from using OutbreakMD. This brief proposes such an application.

Nafasi: A Social Network for Disease Detection

Building off of the innovations made by the Harvard-HealthMap team, this brief proposes a new application—*Nafasi*—that will use crowdsourcing to gather information but will overcome the limitations of the OutbreakMD system. *Nafasi* will:

- Require each doctor to have a registration code to ensure that all reports are reliable and will color code posts to differentiate between those coming from doctors, other health professionals, and independent reporters.

- Integrate with Google Translate, allowing forms to be filled out in 63 languages.

- Use a fill-in form containing fields for patient age range, gender, ethnicity, symptoms, treatment, and prognosis, rather than checkboxes of already reportable diseases.

- Include an optional section in the form for patient address if the patient is being seen by a doctor outside of their place of residence.

- Inform health professionals about potential threats in their areas. This puts doctors on the alert for specific symptoms and will increase compliance by underscoring that contributing information is important to a wider community of health workers.

These modifications will make the application more accessible to public health professionals and make it more difficult to tamper with data input. In addition, there are logistical, financial, and political realities that must be addressed in order to ensure widespread use of *Nafasi*.

Logistical Considerations

- Posting reports to *Nafasi* relies on internet access in rural areas of low-income countries. 11.4% of Africans, 23.8% of Asians, and 36.2% of Latin Americans have internet access.[51]

  Solution: Internet access has grown 480% in the past 10 years, and 2527.4% in Africa. While many areas are still unconnected, this is changing rapidly—even without any additional intervention.[52] During an outbreak, the government could

further improve access by constructing additional cellular phone towers—the fastest and cheapest way to increase wireless access—in isolated affected areas.

- A major hurdle in implementing any new program is spreading awareness. Since crowdsourcing is particularly dependent on mass participation, implementation of *Nafasi* must include a mechanism for education and training.

  Solution: Countries can spread *Nafasi* by requiring schools to educate future health professionals in the use of *Nafasi* during their training, teaching caregivers about the importance of accurate reporting. For health professionals who have completed their education, additional training programs could be held. In addition to training doctors, the implementation of *Nafasi* should begin with a pilot program at the district or province level, which would then spread to other provinces, eventually creating an integrated nationwide system.[53]

Financial Considerations

Nafasi will generate an enormous amount of raw data that must be analyzed.

- Individual countries often cannot afford the high cost of manual analysis, and the WHO does not have the budget or the workforce to integrate and analyze all countries' data.[54]

  Solution: The application uses a standard GETIS-ORD algorithm, which is open source and can be programmed into the application to analyze data. This algorithm looks for hot-spots, defined as areas containing a certain number or proportion of cases. When it detects a cluster of multiple hotspots in the same area, it will trigger an alert.

- Smart phones are expensive. Even if internet access reaches into all areas of developing countries, not all health professionals will be able to access *Nafasi*.

  Solution: Several NGO's are already beginning to distribute smart phones to villagers in remote areas.[55] Elsewhere, purchasing a single internet-capable device per village is an inexpensive commitment for participating countries to make.

The major obstacle for current epidemiological surveillance systems is that information gathering and analysis are prohibitively expensive. By improving internet access and using

GIS-pattern recognition rather than manual analysis to handle raw data, the cost of implementing *Nafasi* will be significantly lower than current systems.

Political Considerations

Crowdsourcing systems have generally faced little political opposition, as they are operated by citizens and not states. But since health professionals in many developing countries are government employees, the cooperation of governments is crucial to the success of *Nafasi*. State participation faces several barriers:

- Any system tied to a U.S.-based actor will be perceived as interference by Washington in a country's domestic affairs, if not outright imperialism. This would severely curtail the willingness of states to participate in the program.

- If information is publicly available, as with traditional crowdsourcing applications, many countries will limit what their public health community is allowed to report, in order to prevent hostile states from taking advantage of internal weaknesses or for fear that news of an outbreak will affect international trade and tourism.

- States may refuse to participate due to a historical unwillingness to share information. For example, the failure to report the SARS outbreak in China indicates a reluctance to cooperate with the international community on such matters or admit to their inability to control the outbreak.[56]

Achieving large-scale cooperation and information sharing among countries is a difficult undertaking that cannot be solved solely by technology. The key to garnering state support for *Nafasi* is a program of implementation that moves gradually from domestic implementation to global partnerships.

Implementation of *Nafasi*: Overcoming Political Barriers Through Gradual Centralization

In order to overcome opposition to information sharing, this brief proposes a three-phase rollout of *Nafasi*.

Phase One: Individual States Adopt *Nafasi*

The lack of accurate information in global epidemiological surveillance stems from two

separate problems: (1) the lack of local surveillance within each country, and (2) hesitation on the part of individual states to report sensitive information to the international community. Phase One will address the first of these problems. During Phase One:

- *Nafasi* will be provided to countries for free with regular updates being made available online, similar to Mozilla's products. It will be available as a website or as an application for Apple products or those with an Android operating system.

- Countries that adopt *Nafasi* will have access only to their own raw data and a *Nafasi*-produced map.

- Each country will be responsible for encouraging the use of *Nafasi* throughout its health system and reacting to any outbreaks detected by the system.

- No information sharing will be required or expected.

Countries will adopt *Nafasi* because it provides a cheap, efficient, and effective means of meeting the demand for improved epidemiological surveillance, and is also in line with the general trend in the global health community of using information technology to improve health.[57] Most developing nations have budgets for improving surveillance using the WHO's health systems building blocks—Zimbabwe spent $75 million on AIDS surveillance in 2010 alone—but have not seen the hoped-for successes.[58]

A country will have completed Phase One when at least 75% of health professionals in rural areas use *Nafasi* regularly to submit information on reportable diseases or suspicious symptoms.

Phase Two: Bilateral Information Sharing

Phase Two will address the fact that epidemics cross borders, and that information sharing by neighbors is necessary to obtain a complete picture of potential outbreaks. There is already a precedent for states to cooperate in the case of an outbreak, so this form of information sharing will occur naturally. In Phase Two:

- States will first sign bilateral information-sharing agreements, followed by multilateral or regional agreements.

- Individual national maps will be combined into a single regional map to which all partners will have access.

- The regional map will be analyzed by GIS algorithms as a whole, rather than by country, and all partners will receive notification of all potential outbreaks within cooperating states.

During outbreaks, even hostile states routinely cooperate on detection and prevention. This precedent is most notably apparent in MECIDS, the longstanding partnership between Israel, the Palestinian Authority, and Jordan to detect and prevent food-borne illnesses. In 2005 and 2009, this infrastructure was used to track and prevent avian and swine flu outbreaks, respectively. The partnership involves a documented plan for each country's responsibilities in the event of a pandemic and has included efforts by Israel to improve lab testing and treatment services for influenza in both the Palestinian Authority and Jordan. [59]

Bilateral agreements have the potential to encourage countries to provide aid to neighbors should an outbreak strike, in the interest of preventing the disease from spreading into their own territory. Over time, it may also increase interdependence between states, giving each partner a vested interest in maintaining the stability of cooperating states.

Phase Three: Centralization

Phase Three will occur in conjunction with Phase Two and will centralize the data gathered by each country's *Nafasi* at the WHO in order to create a global database of information on potential outbreaks. While the WHO is currently undergoing major cutbacks due to loss of funding, managing a global *Nafasi* system would not require additional funds, and could be accomplished by reallocating resources from other information gathering programs made obsolete by *Nafasi*.[60] During Phase Three:

- The WHO will provide incentives for countries to share individual *Nafasi* maps with the WHO, in keeping with their stated commitment to encourage improved epidemiological surveillance.[61] These incentives will include:

    - Aid in the case of an outbreak. This can be done by reallocating the $816 million currently in the 2012-2013 WHO budget for improving surveillance and outbreak response.[62]

    - Improvements on public health infrastructures, such as clinics, laboratory facilities for diagnosis, and health education programs.

- Pressure from other WHO member states during regular meetings. This is the primary means of persuading states to share information currently used by the WHO.[63]

- A global map will be constructed from participating countries' *Nafasi* maps and GIS-analyzed by the WHO.

- Individual countries will *not* have access to the *Nafasi* maps of all countries sharing information with the WHO but will continue to have access to any bilateral or regional maps formed in Phase Two.

- The WHO will not notify individual countries of an outbreak in another country unless there is an information sharing agreement already in place or the WHO deems it impossible to control the outbreak before it crosses international borders.

- WHO representatives and the affected country will both receive a notification in the case of an outbreak.

Phase Three will allow the WHO to ensure that an outbreak has not spread beyond its country of origin and to provide early warning to potentially threatened countries if it appears that a state is unwilling or unable to isolate the outbreak within its borders. Early warning will allow states to take preventative measures, such as closing borders, to protect their populations from disease and their national interests from the instability and conflict that can accompany pandemic disease.

Conclusion

Infectious agents are evolving more rapidly than they have at any point in history, threatening all states with the potential for a global pandemic. Even a moderately infectious disease could kill millions, cause economic collapse as the workforce is decimated, create domestic instability as governments lose the capacity to function, and trigger interstate conflicts as regional balances of power are disrupted by outbreaks in the military. A pandemic cannot be stopped once it has spread across international borders, but it can be prevented at its source. By replacing inefficient, inaccurate epidemiological surveillance systems with a more advanced, cheaper, global network based on cutting edge crowdsourcing technology, outbreaks can be isolated and resources devoted to their control.

[1] Susan Peterson, "Epidemic Disease and National Security," *Security Studies*, 12, no. 2 (2002): 43-81.

[2] Lana Thorpe, Anne Paxton, and James Clarke, "The Future of Global Health: Building Global Capacity," *The Journal of Global Health*, 1, no. 2 (2011): 1-2.
[3] Jeffery Taubenberger, "1918 Influenza: the Mother of All Pandemics," *CDC Historical Review*, 12, no. 1 (2006): 15-22.
[4] For "malaria" see: William Moss, "Measles still has a devastating impact in unvaccinated populations," *PLoS Medicine*, 4, no. 1 (2007): 9-10.
For "polio" see: Centers for Disease Control and Prevention, "CDC Global Health- Polio." Last modified January 6, 2012. http://www.cdc.gov/polio/.
[5] Peterson, "Epidemic Disease and National Security."
[6] Andrew Price-Smith, *Contagion and chaos: disease, ecology, and national security in the era of globlization*, (Boston: MIT University Press, 2009), 78.
[7] Andrew T. Price-Smith, "The Pandemic Influenza of 1918: Implications for Modern Health Governance and International Security" (paper presented to Finnish Institute of International Affairs, Helsinki, May 10, 2011).
[8] Niklas Mackler, William Wilkerson, and Sandro Cinto, "Will First-Responders Show Up for Work During a Pandemic? Lessons From a Smallpox Vaccination Survey of Paramedics," *Disaster Management and Response*, 5, no. 2 (2007): 45-8.
[9] Internal stability would be caused by labor shortages and low productivity. High mortality rates- particularly in adults- and dramatically lower income create a generation of poverty-stricken, homeless, uneducated orphans who are significantly more likely to be tempted by violent crime or the promises of radicalism
[10] Elizabeth Lule, and Markus Haacker, *The Fiscal Dimension of HIV/AIDS in Botswana, South Africa, Swaziland, and Uganda*, (Washington, D.C.: The World Bank, 2012), 128.
[11] U.S. Library of Congress. Congressional Research Service. *South Africa: Current Issues and U.S. Relations* by Lauren Ploch. Washington: The Service, 2011.
[12] Vaccine development for a new strain of influenza- the best case scenario, as a protocol for vaccine creation already exists- would take 3-6 months, and producing enough vaccines for the entire global population would take 2-3 years, with all factories working at full capacity (Lee and Fidler, 2007).
[13] The fourteen largest vaccine production factories produce 90% of the supply; these factories are all in OECD high income countries (European Vaccine Manufacturers, Worldwide Major Vaccine Manufacturers in Figures, 2004, p.1, from EVM Website, http://www.evm-vaccines.org/pdfs/mfrs_in_figures.pdf, Accessed January 16, 2012.)
[14] Edward Hammond. "Indonesia fights to change WHO rules on flu vaccines." *Seedling*, April 18, 2009, 24-32.
[15] *Ibid.*
[16] Richard Thompson and Gregory Hartl. World Health Organization, "Indonesia to resume sharing H5N1 avian influenza virus samples following a WHO meeting in Jakarta." Last modified March 27, 2007. http://www.who.int/mediacentre/news/releases/2007/pr09/en/index.html.
[17] Most refugees would be relatively poor and will not travel long distances, so neighboring countries would bear most of the economic burden of supporting refugee populations.
For migration and interstate conflict, see: Joakim Gundel. "The Migration-Development Nexus:Somalia Case Study." *International Migration*. 40. no. 5 (2003): 255-281.
[18] Brandon Valeriano. "When Does Migration Lead to Interstate Conflict? ." *Presented and Prepared for the International Studies Association Annual Meeting*. (2012).
[19] For growing tensions see: Congressional Research Service. *South Africa: Current Issues and U.S. Relations* by Lauren Ploch.
For violence against refugees see: Doctors Without Borders, "Beyond Cholera: Zimbabwe's Worsening Crisis." Last modified February 17, 2009. Accessed February 25, 2012. http://www.doctorswithoutborders.org/publications/article.cfm?id=3408&cat=special-report.
[20] Sharhbanou Tadjbakhsh, and Anuradha Chenoy, *Human Security: Concepts and Implications*, (New York, NY: Routledge, 2007), 114.
[21] Bernard Choi, "Perspectives on Epidemiologic Surveillance in the 21st Century," *Chronic Diseases in Canada*, 19, no. 4 (1998): 145-151.
[22] Kate Jones, Nikkita Patel, Marc Levy, Adam Storeygard, Deborah Balk, John Gittleman, and Peter Dazsak, "Global trends in emerging infectious diseases," *Nature*, 451 (2008): 990-993.
[23]Peter Nsubuga, Mark E. White, Stephen B. Thacker, Mark A. Anderson, Stephen B. Blount, Claire V. Broome, Tom M. Chiller, Victoria Espitia, Rubina Imtiaz, Dan Sosin, Donna F. Stroup, Robert V. Tauxe, Maya Vijayaraghavan, and Murray Trostle, *Disease Control Priorities in Developing Countries.*, (Washington, D.C.: World Bank, 2006), chap. 53.

[24] Centers for Disease Control and Prevention, "Office of Surveillance, Epidemiology, and Laboratory Services." Last modified July 15,2011. Accessed February 14, 2012. http://www.cdc.gov/osels/.
[25] Centers for Disease Control and Prevention, "National Center for Emerging and Zoonotic Infectious Diseases." Last modified January 26, 2012. Accessed February 14, 2012. www.cdc.gov/ncezid/index.html.
[26] Centers for Disease Control and Prevention, "Office of Public Health Preparedness and Response." Last modified March 9, 2012. Accessed February 14, 2012. http://www.cdc.gov/phpr/about.htm.
[27] Ralph Frerichs, "Epidemiological Surveillance in Developing Countries," *Annual Review of Public Health*, 12 (1991): 257-90.
[28] *Ibid*.
[29]The budget for OSELS in FY2011 was $237,747,000. The budget for the NCEZID was $304,193,000, and the budget for PHPR was $1,415,416,000. Centers for Disease Control and Prevention, *Fiscal Year 2011 Operating Plan Table* (Washington, D.C., 2011), 1.
[30] Frerichs, "Epidemiological Surveillance in Developing Countries," pp. 257-90.
[31] *Ibid.*
[32] Jane Falkingham, "Poverty, out-of-pocket payments and access to health care: evidence from Tajikistan," *Social Science & Medicine*, 58, no. 2 (2004): 247-58.
[33] In a typical system in South Asia, Myanmar's primarily paper-based system, health professionals are required to fill out 30 forms per day and an additional form with 1,946 variables at the end of each month (Frerichs, 1985).
[34] Frerichs, "Epidemiological Surveillance in Developing Countries," pp. 257-90.
[35] Centers for Disease Control and Prevention, "Global Health - Global Disease Detection and Emergency Response." Last modified July 19,2011. Accessed March 14, 2012. http://www.cdc.gov/globalhealth/gdder/.
[36] Epidemiologists are trained according to the same guidelines used by the CDC's Epidemic Intelligence Service.
[37] Centers for Disease Control and Prevention, "Integrated Disease Surveillance and Response." Last modified April 16,2008. Accessed March 14, 2012. http://www.cdc.gov/idsr/.
[38] Lawrence Madoff, "ProMED-mail: An Early Warning System for Infectious Diseases ," *Clinical Infectious Diseases*, 39 (2004): 227-32.
[39] International Society for Infectious Diseases, "About ProMED-mail." Accessed March 14, 2012. http://www.promedmail.org/aboutus/.
[40] Pamela Johnson and David Blazes. "Using Cell Phone Technology for Infectious Disease Surveillance in Low-Resource Environments: A Case Study from Peru" in *Global Infectious Disease Surveillance and Detection: Assessing the Challenges – Finding Solutions, Workshop Summary,"* eds. Stanley M. Lemon, Margaret A. Hamburg, P. Frederick Sparling, Eileen R. Choffnes, and Alison Mack (Washington D.C.: National Academies Press, 2007), 136-52.
[41] Crowdsourcing technology has since been used to track earthquake damage in Haiti and crime in Atlanta, GA using the Kenyan-based platform Ushahidi, and has also been used by Amnesty International to track human rights abuses.
[42]. John Brownstein, Clark Frieifeld, Ben Reis, and Kenneth Mandl. "HealthMap: Internet Based Emerging Infectious Disease Intelligence" in *Global Infectious Disease Surveillance and Detection: Assessing the Challenges – Finding Solutions, Workshop Summary,"* eds. Stanley M. Lemon, Margaret A. Hamburg, P. Frederick Sparling, Eileen R. Choffnes, and Alison Mack (Washington D.C.: National Academies Press, 2007), 136-52
[43] Rumi Chunara, Clark Freifeld, and John Brownstein, "OutbreakMD: tracking and identifying outbreaks in post-earthquake Haiti," *Emerging Health Threats Journal*, 4 (2011): s12-13.
[44] Children's Hospital Boston, "About HealthMap." Accessed February 26, 2012. http://www.healthmap.org/en/.
[45] Clark Freifeld, *Participatory Epidemiology: Harnessing the HealthMap Platform for Community-Based Disease Outbreak Monitoring.* MA thesis, Massachusetts Institute of Technology. Boston, MA: MIT University Press, May 7, 2010.
[46] Brownstein, John. HealthMap, "OutbreakMD." Accessed February 1, 2012. http://healthmap.org/outbreakmd/.
[47] Jeffrey Shields, (Professor of Biology at the College of William and Mary, Parasitology Specialist), interview by Efrat Rosenzweig, "Obstacles to Improved Surveillance in the Developing World," February 07, 2012.
[48] *Ibid*.
[49] Children's Hospital Boston, "About HealthMap." Accessed February 26, 2012. http://www.healthmap.org/en/.
[50] Brownstein, John, "OutbreakMD." http://healthmap.org/outbreakmd/.
[51] European Travel Commission, "World Usage Patterns ." Last modified March 7, 2012. http://www.newmediatrendwatch.com/world-overview/34-world-usage-patterns-and-demographics.
[52] *Ibid*.

[53] Patricia A. Abbott, (Co-Director of the PAO/WHO Center for Knowledge Management), interview by Efrat Rosenzweig, "Capacity of WHO to Manage Phase Three," March 06, 2012.
[54] World Health Organization, *Programme Budget 2012-2013*, (Geneva, 2011). Accessed March 01, 2012. http://whqlibdoc.who.int/pb/2012-2013/PB_2012%E2%80%932013_eng.pdf.
[55] Banks, Ken. "From smart phones to smart farming: Indigenous knowledge sharing in Tanzania." November 30, 2011. http://newswatch.nationalgeographic.com/2011/11/30/smart-phones-meet-smart-farming-indigenous-knowledge-sharing-in-tanzania/ (accessed).
[56] Normile Enserink, "SARS in China. Tracking the roots of a killer." (2003): 297-9,
[57] Eric Goosby, "PEPFAR committed to mobile health solutions," *Global Health Matters*, 11, no. 1 (2012). And Peter Nsubuga, Okey Nwanyanwu, John Nkengasong, David Mukanga, and Murray Trostle, "Strengthening public health surveillance and response using the health systems strengthening agenda in developing countries" (2012): S1-5.
[58] Zimbabwe National AIDS Council and Ministry of Health and Child Welfare, *Zimbabwe National HIV and AIDS Strategic Plan (ZNASP) 2006-2010*, (Harare, 2006) Accessed March 04, 2012. http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_125613.pdf
[59] William J. Long, *Pandemics and Peace: Public Health Cooperation in Zones of Conflict*, (Washington, D.C.: United States Institute of Peace Press, 2011), 30-39.
[60] Patricia A. Abbot, interview by Efrat Rosenzweig, March 06, 2012.
[61] The World Health Organization, *Strategic Enhancement of Laboratory and Epidemiology Surveillance*, (Leon, 2003). Accessed March 03, 2012. http://www.who.int/csr/disease/Anthrax/PhilippeDuboisa.pdf.
[62] World Health Organization, *Programme Budget 2012-2013*.
[63] Patricia A. Abbot, interview by Efrat Rosenzweig, March 06, 2012.

P|I|P|S *The Project on International Peace and Security*

2011-2012 RESEARCH FELLOWS

ALLISON BAER, CLASS OF 2013

"Educational Reform and Information Technology: Combating Radicalism in Pakistan"

BENJAMIN BUCH, CLASS OF 2012

"The Active Denial System: Obstacles and Promise"

PETER KLICKER, CLASS OF 2012

"A New 'Freedom' Fighter: Building on the T-X Competition"

KATHERINE MITCHELL, CLASS OF 2013

"The Active Denial System: Obstacles and Promise"

EMILY PEHRSSON, CLASS OF 2013

"Making the Grade: An International Regulatory Framework for Cybersecurity"

EFRAT ROSENZWEIG, CLASS OF 2012

"Crowdsourcing Global Security: Fighting Pandemic Disease in the Information Age"

P|I|P|S *The Project on International Peace and Security*

2011-2012 RESEARCH INTERNS

BRIANNA BUCH, CLASS OF 2015

"Crowdsourcing Global Security: Fighting Pandemic Disease in the Information Age"

MICHAEL CAMPBELL, CLASS OF 2015

"A New 'Freedom' Fighter: Building on the T-X Competition"

LOGAN FERRELL, CLASS OF 2015

"The Active Denial System: Obstacles and Promise"

DALLEN MCNERNEY, CLASS OF 2014

"Educational Reform and Information Technology: Combating Radicalism in Pakistan"

CONNOR SMITH, CLASS OF 2014

"The Active Denial System: Obstacles and Promise"

JIMMY ZHANG, CLASS OF 2015

"Making the Grade: An International Regulatory Framework for Cybersecurity"