LBJ Journal of Public Affairs

Volume 20 2012

The *LBJ Journal of Public Affairs* (ISSN 1087-268X) is produced by students of the LBJ School of Public Affairs at The University of Texas at Austin. Founded in 1989, it is one of the nation's oldest student-run journals of public affairs. The *LBJ Journal* is dedicated to publishing professional quality work by the extended LBJ School community, promoting discourse on contemporary policy issues, and enhancing the reputation of the LBJ School of Public Affairs. President Lyndon B. Johnson believed that through collective discussion and action the needs of people could be met; likewise, the *LBJ Journal* believes that as a result of diverse and vigorous discourse about public affairs, policies are created and initiatives are taken that best serve the interest of citizens everywhere.

Drawer Y, University Station, Austin, Texas 78713-8925
Phone: 512-471-3200
Fax: 512-471-8455
lbjjpa@uts.cc.utexas.edu
www.lbjjournal.com

Table of Contents

Editors' Foreword

THIS HAS BEEN AN EXCITING YEAR FOR THE LBJ JOURNAL. For the first time in recent history, an editorial board was selected to assist with the production of the journal. Their hard work and dedication throughout the entire publication process was instrumental in the journal's production.

This volume of the journal represents a wide range of topics that are both timely and of great significance in the public policy realm. Todd Smith explores sustainable development in South Africa; Jessica Brown and Rian Carkhum analyze value-added accountability in Texas; and Marc Olivier examines cyber warfare.

We are grateful to the LBJ School faculty, staff and the Graduate Public Affairs Council (GPAC) for their continued support of the journal. We would also like to thank Dr. Robert Wilson for serving as the LBJ Journal's faculty advisor. Finally, the members of last year's leadership team deserve a great deal of thanks and recognition for their hard work.

Accountability and Equity in the Texas Public School System

Jessica A. Brown, jayannbrown@gmail.com
Rian K. Carkhum, rian.carkhum@gmail.com
University of Texas at Austin

Abstract

Underlying popular use of accountability policies are two assumptions, one of raising academic achievement and another of providing opportunities for equity. As accountability policies grow in complexity, it is necessary to evaluate them according to these assumptions. This study examines one particular addition, the use of growth models in Texas known as the Texas Projected Measure (TPM). Findings suggest that the application of TPM allowed certain schools to move up in accountability ratings. This diluted the traditional conceptions of achievement while also concentrating disadvantaged students into lower accountability rating groups. Growth models such as these need to be further scrutinized as they may not be appropriate for articulating actual achievement and may hinder schools' ability to provide equal opportunities to their students.

Value-Added Accountability: Understanding Equity and the Use of Projection Measures in the Texas Accountability Ratings

Today's educational reform agenda is driven by accountability measures that examine standardized testing and school ratings. The push for the accountability movement has two inherent assumptions behind it: it will provide for greater student achievement and greater equity in schooling.[1] The achievement assumption is based on the idea that testing will allow schools to gauge and change instruction to yield greater attainment measured by standardized tests. The equity assumption emerges from the idea that explicitly focusing on disadvantaged subpopulations will force schools to acknowledge achievement gaps and work to increase equity between student subpopulations.

The extant body of research on achievement and accountability suggests that state and federal accountability systems are connected with improved overall student achievement.[2] However, the research on equity and accountability often argues that accountability practices are not connected with greater opportunities for equity.[3] The research suggests that the use of accountability policies may further exacerbate inequality by disproportionately placing disadvantaged students into schools rated as failing, subjecting them to the negative consequences of sanctions.[4] This debate illuminates the need for continual evaluation of accountability policies in order to ensure they meet the demands and assumptions behind them. Conscientious evaluation is made more challenging by the increasing specificity included in the ever-changing accountability policies themselves.

This study examines one particular example of a complex addition in accountability policy, the use of value added, or growth, models in Texas known as the Texas Projected Measure (TPM). This measure was a unique type of growth model that calculated the growth from one year to the next and used that calculation to predict future success on standardized achievement tests. These projections were used to move schools into a higher state accountability rating group than they would have been assigned absent the growth model. Touted as a more precise measure of student performance, the TPM added another layer of intricacy to measuring student achievement, making it more difficult to fully understand the components of school ratings and what they said about schools deemed as failing.

Under the assumption that failing accountability ratings and sanctions hinder opportunities for equity, this study explores how the addition of growth models found in the TPM affected which types of students were exposed to such sanctions. Findings from our research suggest that with the application of TPM, the lower limit of each accountability rating group decreased, making it possible for certain schools to have lower test scores but be rated in a higher category. The addition of the TPM also influenced equity by concentrating subpopulations of students that were economically disadvantaged, minority, or Limited English Proficient (LEP) into the failing group. This suggests that while the TPM allowed for more campuses to attain acceptable ratings, it also left certain types of student behind, exposing a number of minority and disadvantaged students left in failing schools to sanctions that could restrict them from attaining the same level of achievement as their peers.[5] This concentration may hinder opportunities for equity suggesting that the use of the TPM does not meet the assumptions behind the accountability movement.

These findings are in line with negative public opinion on the use of TPM and growth models in accountability policies.[6] Citing this lack of support, the Commissioner of education in Texas recently reported that schools will no longer be rated using TPM.[7] We contend that, as the use of TPM contributed to further stratification of subpopulations of students, the suspension of this policy is a small step in providing for more equitable components in the state accountability rating program. These findings suggest that specific attention must be paid to specific accountability procedures to ensure continual evaluation of these policies and how well they meet the assumptions of both achievement and equity.

REVIEW OF THE LITERATURE

In recent decades, the focus of accountability has shifted from input measures to output measures.[8] The theory behind this shift implies that by allowing districts and schools more freedom with their input resources, they will use them creatively to reach set output measures.[9] These outputs are often defined under accountability standards that measure a school's growth toward a preset expectation level. The output measures used most often are standardized tests. Students take a state level test, which measures a campus' performance by how many students pass a fixed level. By focusing on outputs, accountability measures are touted as a way to easily grade schools and identify those in need of further scrutiny.

In the United States, the use of accountability policies has two inherent assumptions: they will raise student achievement and ensure equity between different types of students.[10] These assumptions have helped to popularize accountability and driven legislative change toward inclusion of accountability practices at all levels.[11] As such, these two assumptions are critical to the movement and should drive research and evaluation on every accountability policy.

The prevailing body of research suggests that accountability practices may indeed raise student achievement. A meta-analysis, stemming from 14 studies examining the effect of high stakes testing on student achievement, found that high-stakes accountability practices have had a modestly positive effect on learning.[12] Using Texas accountability practices specifically, several studies have also found positive links between the policy and student achievement.[13]

While the research on raising student achievement suggests positive effects, research on accountability and equity evinces a more negative picture. Most of the current research indicates that the practices do not lead to greater opportunities or increased equity for traditionally disadvantaged subpopulations of students.[14] Even in studies which do demonstrate growth in achievement according to tests, there has been no link between accountability practices and narrowing of gaps between these disadvantaged subpopulations and their higher achieving peers.[15] Additionally, there are indications that accountability actually endangers certain students. One such study outlines how accountability practices hamper high poverty and racially diverse schools because they have to meet the same standards as their more affluent peers based on test scores that do not control for student characteristics.[16] As such, students in these schools are subject to state and federal sanctions and/or reconstitution which may further compromise their educational opportunities.[17]

The research to date has yielded, at best, an inconsistent view as to whether the assumptions driving accountability are being supported through existing policies. While there is an imperative need for more research on these policies, the policies themselves continue to change and evolve, making it ever more difficult to ascertain the actual benefit or harm of these measures on both achievement and equity. One of these policy evolutions that cloud the effects of accountability measures includes the use of value-added, or growth modeling, in the ways which states, such as Texas, rate schools as acceptable or failing.

The Texas accountability model includes four rating groups: Unacceptable, Acceptable, Recognized, and Exemplary. These ratings are based on student test scores, completion rates, and dropout rates.[18] Texas recently experimented with the calculation of these ratings by adding a growth-modeling program to its formula, the Texas Projection Measure.[19] The TPM was calculated using the schools' and students' current test scores to predict whether or not they would pass the Texas Assessment of Knowledge and Skills (TAKS) on future high-stakes test years.[20] Used first in the 2008-2009 school year, the TPM allowed certain schools to gain a higher rating based on these prediction calculations if enough students on the campus were projected to pass TAKS in the next high-stakes year. As a result, 2,560 of over 7,000 Texas public schools used the TPM to raise their accountability rating.[21]

METHODS

The change in ratings for so many schools is the impetus of this study, which evaluates the TPM policy according to both achievement and equity assumptions. Accordingly, this study explores differences in schools' ratings before and after the application of the TPM measure. Two research questions are explored:

> Q_1: How does the distribution of achievement scores between rating groups change with the application of TPM?
>
> Q_2: How does the distribution of student characteristics between rating groups change with the application of TPM?

We expect that if TPM is working as designed, there will be differences in achievement scores between rating groups after the application of the growth measure, creating lower limits in passing rates for each group as campuses with lower scores move up into a higher rating group. Additionally though, we expect that the movement in achievement scores will also correspond to a change the mean student characteristics of each rating group which disproportionately concentrates disadvantaged students in lower rated groups.

This study uses data collected by the state of Texas under the Academic Excellence Indicator System (AEIS) and the Accountability Rating System for Texas Public Schools and Districts for the 2008-2009 school year. This data represents the first full year of TPM implementation; it contains school-level information on student demographics, school characteristics, and accountability measures. Data for comprehensive high schools, those serving grades 9-12, were used for analysis after eliminating charter schools and juvenile detention or other special schools with missing accountability information (n=978). As high schools often concentrate students from a wider number of feeder schools, these campuses are expected to have larger numbers of student in subpopulations which are counted under the state accountability rating system.

Schools were first organized into rating groups without the inclusion of the TPM growth model; in analysis this is identified as "pre-TPM." Schools were also ranked into rating groups with the inclusion of the growth measure; this is identi-

fied as "post-TPM." In sum, 483 of the 978 schools (49 percent) used the TPM to improve their accountability rating. More specifically, 117 schools used TPM to achieve academically Acceptable, 302 to achieve Recognized, and 62 to achieve an Exemplary rating.

Our analysis consisted of running 14 one-way Analysis of Variances (ANOVAs) for both pre-TPM and post-TPM ratings on a number of achievement and student characteristics. Accountability characteristics include the percentage of all students passing the English Language Arts (ELA), mathematics, social studies, and science TAKS test across all grades. Student characteristics include the percent of economically disadvantaged students measured in proxy by the percentage of students who received free or reduced lunch prices. In addition, the summed percentage of traditionally considered minority students at a campus and the percentage of Limited English Proficient (LEP) as measured by the home language survey are also included.

The ANOVA analyses were used to examine the relationship between the four ratings, and also created mean differences for comparison between the pre-TPM and post-TPM rating groups. The *Dunnett's T3* post hoc test was selected in some cases for additional analysis as a conservative measure accounting for unequal variances and lower sample sizes. These post hoc analyses showed where the significant differences occurred between rating groups using the various characteristics tested. All analyses were subject to a preset alpha level of 95 percent confidence ($\alpha = .05$).

FINDINGS

Concurrent with the expectations under our first research question, the TPM was found to boost some schools into higher rating groups, which in turn lowered the range limit of percent passing scores for each group. As would be expected by a ranking system, mean percent passing scores ascended with each rating level where the Unacceptable group had the lowest mean score. This trend did not change with the application of TPM but the mean passing scores for all groups decreased. This suggests that the TPM raised schools' accountability ratings for those just below the benchmark under traditional methods of rating. When looking at the second research question, mean percentage scores for economically disadvantaged, high minority, and Limited English Proficient (LEP) students decreased as accountability ratings increased, except within the Exemplary group. The addition of the TPM further concentrated high levels of these students into the Unacceptable group, thereby exposing them to possible accountability sanctions, as these schools were considered to be failing. Below is a more comprehensive review of the significant findings.

ACHIEVEMENT CHARACTERISTICS

Texas accountability ratings rely on four different TAKS tests for high schools: English Language Arts (ELA), Mathematics, Social Studies, and Science. As part of the analysis, the percentage of all students passing each test across grade levels at

a school were organized according to each accountability rating group. This was completed for both pre-TPM and post-TPM ratings.[22]

For the ELA TAKS, there were significant differences both pre- and post-TPM, $F(3,983)=152.68$, $p<.05$ and $F(3,983)=212.00$, $p<.05$ respectively. As indicated in Table 1, the average percentage passing in each category, Pre-TPM rose as ratings increased, but post-TPM the average percentage passing in all categories decreased. As also indicated in Table 1, the addition of the TPM decreased the lower limit of range scores for the Acceptable, Recognized, and Exemplary rating groups. Post hoc analysis found that the mean differences of each rating group were significantly different from each other; this did not change with the addition of the TPM. This result was consistent throughout each subject tested and suggests that the accountability rating groups, both pre- and post- TPM represented distinct groups of schools which showed significantly different levels of academic achievement.

Math TAKS scores behaved similar to ELA TAKS scores but had lower averages overall and contained an interesting comparison when looking at the change in range for the rating groups with the application of the growth model. Pre- and post-TPM the rating levels were significantly different from each other ($F(3,983)=349.55$, $p<.05$) and the difference remained constant after the application of the TPM, $F(3,983)=345.60$, $p<.05$. The addition of the TPM decreased means across all categories and decreased the lower threshold for the Acceptable, Recognized, and Exemplary ratings (see Table 2). While the mean scores before and after the application of TPM did not change dramatically, the range of scores did (see Table 2). For example, pre-TPM the lower limit for the Exemplary group was 92 percent passing but dropped to 78 percent passing post-TPM. Similarly, the Recognized group went from 73 to 58 percent in the lower range limit pre- and

Table 1
Means by Accountability Rating for Percent Passing ELA TAKS, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Range	Pre-TPM Mean	Post-TPM Mean	Post-TPM Range	Post-TPM n
Unacceptable	184	65-99	86.62 (5.96)	84.46 (6.39)	65-96	67
Acceptable	600	74-99	91.76 (4.36)	89.3 (4.84)	71-99	415
Recognized	181	84-99	95.92 (2.99)	94.06 (3.34)	81-99	421
Exemplary	22	96-99	98.86 (0.64)	97.69 (1.93)	92-99	84
Total	987	65-99	91.72 (5.39)	91.72 (5.39)	65-99	987

Note: Standard deviations are presented in parentheses.

Table 2
Means by Accountability Rating for Percent Passing Mathematics TAKS, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Range	Pre-TPM Mean	Post-TPM Mean	Post-TPM Range	Post-TPM n
Unacceptable	184	35-82	60.22 (9.94)	57.76 (11.03)	35-82	67
Acceptable	600	47-93	73.41 (8.32)	67.54 (9.32)	38-93	415
Recognized	181	73-96	85.44 (5.71)	78.73 (6.91)	58-96	421
Exemplary	22	92-99	96.59 (2.59)	91.35 (4.88)	78-99	84
Total	987	35-99	73.67 (11.72)	73.67 (11.72)	35-99	987

Note: Standard deviations are presented in parentheses.

post-TPM, respectively. In addition, the application of TPM decreased the lower threshold of the Acceptable group from 47 to 38 percent, meaning that if only 38 percent of students passed the math TAKS—only 3 percent higher than the lower limit of the Unacceptable group—a school could still be considered Acceptable (see Table 2). The large drops in the lower range limits and the differences between them suggest that schools with less than desirable math scores were able to attain higher and higher accountability ratings.

Social Studies TAKS had similar results to the ELA TAKS. Pre-TPM rating levels were significantly different from each other, $F(3,982)=165.55$ $p<.05$. Post-TPM rating levels were also significantly different, $F(3,982)=174.34$, $p<.05$. Means, standard deviations, and ranges for these levels can all be found in Table 3.

Lastly, Science TAKS followed the form all other tests in its significant differences both pre- and post-TPM, $F(3,982)=244.77$, $p<.05$ and $F(3,982)=264.33$, $p<.05$, respectively. Range and mean information for Science TAKS can be found in Table 4. The range differences in science scores were similar to those found for math. This was especially seen in the Exemplary category, which dropped the lower range limit from 93 percent pre-TPM to 79 percent post-TPM.

STUDENT CHARACTERISTICS

We expected achievement scores to vary for each group, but we also found that ratings varied for different student characteristics traditionally viewed as disadvantaged. The percentages of economically disadvantaged students, minority students, and Limited English Proficient (LEP) students, were all found to be statisti-

Table 3
Means by Accountability Rating for Percent Passing Social Studies TAKS, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Range	Pre-TPM Mean	Post-TPM Mean	Post-TPM Range	Post-TPM n
Unacceptable	183	60-97	89.10 (5.23)	87.77 (6.22)	60-97	66
Acceptable	600	78-99	93.82 (3.40)	91.86 (3.99)	77-99	415
Recognized	181	88-99	96.99 (2.21)	95.39 (2.81)	80-99	421
Exemplary	22	99-99	99.00 (0.00)	98.27 (1.27)	94-99	84
Total	986	60-99	93.64 (4.42)	93.74 (4.42)	60-99	986

Note: Standard deviations are presented in parentheses.

cally significant pre- and post-TPM. The percentage of disadvantaged students in schools decreased as ratings increased in all but the Exemplary group.

The percentage of economically disadvantaged students was linked to accountability ratings even before the addition of a growth measure. Pre-TPM ANO-

Table 4
Means by Accountability Rating for Percent Passing Science TAKS, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Range	Pre-TPM Mean	Post-TPM Mean	Post-TPM Range	Post-TPM n
Unacceptable	183	38-86	64.11 (10.89)	61.59 (12.52)	38-84	66
Acceptable	600	51-95	75.52 (8.97)	70.07 (9.54)	44-95	415
Recognized	181	70-98	86.76 (5.64)	80.81 (7.41)	60-96	421
Exemplary	22	93-99	96.82 (2.22)	91.80 (5.05)	79-99	84
Total	986	38-99	75.94 (11.58)	75.94 (11.58)	38-99	986

Note: Standard deviations are presented in parentheses.

VA analysis shows that there were significant differences between the rating levels, $F(3,983)=3.16$, $p<.05$. The percentage of economically disadvantaged students for each level significantly decreased as the accountability rating increased, except for the Exemplary group, which had rates similar to the Unacceptable group.

With the application of the growth measure though, the differences in the percent of economically disadvantaged students was more defined. Post-TPM analysis revealed that there were significant differences between the accountability ratings, $F(3,983)=3.83$, $p<.05$. Post-TPM, the average percentage of economically disadvantaged students decreased with each increase in accountability rating. As the rating rose the number of poor students decreased (see Table 5). In the Post-TPM ANOVA, post hoc analysis revealed more defined differences; the Unacceptable group was found to be significantly different from all other groups. The mean difference between Unacceptable to Acceptable was 10.17, Unacceptable to Recognized was 11.85, and Unacceptable to Exemplary was 12.12, $p< .05$. None of the other groups were significantly different from each other. This supports the notion that TPM concentrated more economically disadvantaged students into the Unacceptable group where their schools were subject to state sanctions.

Analyses on the percentage of minority students showed similar trends but differing levels of significance (see Table 6). Pre-TPM, the groups were significantly different from each other, $F(3,983)=3.62$, $p<.05$. In this category, Exemplary schools had the most minority students, then Unacceptable campuses, followed by Acceptable, and Recognized. Post-TPM analysis showed that the groupings were not significantly different but trended towards significance, $F(3,983)=2.57$, $p=.053$. The means for both the Acceptable and Recognized groups showed an increase, consistent with the idea that diverse schools were able to move up in ranking, but

Table 5
Means by Accountability Rating for Percent Economically Disadvantaged, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Mean	Post-TPM Mean	Post-TPM n
Unacceptable	184	63.46 (27.67)	69.01 (28.26)	67
Acceptable	600	58.01 (26.87)	58.84 (26.11)	415
Recognized	181	55.32 (27.06)	57.16 (27.84)	421
Exemplary	22	63.11 (26.64)	56.89 (26.26)	84
Total	987	58.64 (27.14)	58.64 (27.14)	987

Note: Standard deviations are presented in parentheses.

Table 6
Means by Accountability Rating for Percent Minority Students, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Mean	Post-TPM Mean	Post-TPM n
Unacceptable	184	67.84 (30.35)	72.28 (28.94)	67
Acceptable	600	61.97 (30.94)	62.77 (30.43)	415
Recognized	181	58.50 (29.93)	61.12 (30.96)	421
Exemplary	22	71.73 (28.01)	61.98 (31.35)	84
Total	987	62.65 (30.71)	62.65 (30.71)	987

Note. Standard deviations are presented in parentheses.

the Exemplary group showed a decrease which indicates that schools with less diversity were those who moved from Recognized to Exemplary, the most elite rating group. At the same time, the Unacceptable group grew by roughly 5 percent signifying that students left in failing schools were more likely to be students of color.

Pre-TPM the percentage of LEP students was not found to be significantly different across ratings, pre-TPM, $F(3,983)=.296$, $p=.83$. The mean averages for LEP students pre-TPM decreased as accountability ratings increased (see Table 7). However post-TPM, LEP mean percentages were significantly different across the groups, $F(3,983)=3.63$, $p<.05$. The application of the TPM led to an increase in the percentage of LEP students in the Unacceptable, Recognized, and Exemplary schools, but a very slight decrease in the Acceptable schools (see Table 7). Overall, the post-TPM means suggest that the schools were not promoted by the TPM are the ones with larger numbers of LEP students, again suggesting that the TPM is concentrating disadvantaged students into schools with sanctions.

DISCUSSION

In line with our expectations, the TPM did shift schools into higher groups than their test scores would have previously mandated. The application of this growth model also redistributed the schools, changing the demographic makeup in each rating group with disadvantaged students being even more concentrated into the Unacceptable rating and more likely subject to sanctions that would further impede opportunities for academic success and equity.

Table 7
Means by Accountability Rating for Percent LEP Students, Pre– and Post–TPM

Rating	Pre-TPM n	Pre-TPM Mean	Post-TPM Mean	Post-TPM n
Unacceptable	184	16.10 (18.75)	20.94 (23.17)	67
Acceptable	600	14.66 (18.83)	13.27 (16.72)	415
Recognized	181	14.83 (18.69)	15.66 (19.84)	421
Exemplary	22	14.16 (15.57)	14.90 (17.32)	84
Total	987	14.95 (18.71)	14.95 (18.71)	987

Note: Standard deviations are presented in parentheses.

We found that the application of the TPM did little to raise up actual academic achievement as it just reordered schools and gave them higher rating labels. This did not mean that schools performed on a higher scale but rather that the TPM watered down what it meant to be rated as Acceptable, Recognized, or Exemplary. This was especially true in the case of math and science where the lower limit of passing scores dropped dramatically and were well below what would traditionally be considered a mark of exceeding achievement. Further, because most schools using the TPM were already considered to have satisfactory levels of achievement, but used the growth model to gain an even higher rating, our findings suggest that the TPM was not an appropriate tool to move schools out of failing status or away from sanctions.

Added to this effect that the TPM had on reorganizing the schools based on academic achievement, it also had a negative effect on the distribution of disadvantaged students across the rating groups. The application of the TPM advanced certain schools while leaving others behind. We recognized that the TPM did allow for 64 percent of schools to leave the failing status for academically Acceptable, but our findings suggest that the most vulnerable students were left behind in failing schools where sanctions would limit equity efforts.

The distribution of student characteristics may even be more stark than our findings suggest. When cleaning the data, we were unable to censor magnet schools within the larger high school set. Anecdotally, we are aware of several high performing magnets which recruit high-achieving students from disadvantaged backgrounds. As the state does not disaggregate schools by this school type, we were unable to pull out these programs from the full data. As such, the high levels

of minority and economically disadvantaged students in the Exemplary category may be misrepresentative of actual comprehensive high schools. We would expect that without the magnet programs' inclusion, the distribution of schools across rating categories would be inversely related to the number of disadvantaged students. This would paint a far more dismal picture of what high achieving in Texas looks like.

In April 2011 the Commissioner of Education reported that the state will discontinue use of the TPM, but the model has already left its mark.[23] Due to the application of this growth model, some schools have changed their accountability rating while others have been unable to do so. A number of these schools have either escaped sanctions or been left in the failing group and subject to them. Concurrent with our findings, the discontinuance of the TPM is appropriate as it did nothing to increase actual student achievement and may have negatively impacted disadvantaged students creating fewer opportunities for equity. While the break from TPM has already lent way to another iteration of complex accountability policies in Texas, the findings from this specific procedure support the need to continual evaluation of these policies in order to check the assumptions of accountability which drive them. This is especially true in the current political context as the federal government has yet to abandon the notion of growth modeling and has included it in the recent ESEA reauthorization "blueprint" from the Obama administration.[24] As we move forward with these accountability policies and practices, it is imperative to juxtapose new recommendations for measuring student and school performance with their effect on both academic success and opportunities for equity.

ENDNOTES

1. K.A. McDermott, "Expanding the Moral Community or Blaming the Victim? The Politics of State Education Accountability Policy," *American Education Research Journal* 44,1 (2007): 702-709; D. Hursh, "The Growth of High-Stakes Testing in the USA: Accountability, Markets and the Decline in Educational Inequality," *British Educational Research Journal* 31,5 (2005): 605-622; and L.D. Fusarelli, "The Potential Impact of the No Child Left Behind Act on Equity and Diversity in American Education," *Educational Policy* 18, 71 (2004): 72-94.

2. J. Lee, "Is Test-Driven External Accountability Effective? Synthesizing the Evidence From Cross-State Causal-Comparative and Correlational Studies," *Review of Educational Research 78,*3 (2008): 608-644; E.A. Hanushek and M.E. Raymond, "The Effect of School Accountability Systems on the Level and Distribution of Student Achievement," *Journal of the European Economic Association* 2,2/3 (2004): 406-415; and M. Carnoy and S. Loeb, "Does External Accountability Affect Student Outcomes? A Cross- State Analysis," *Educational Evaluation and Policy Analysis* 24,4 (2002): 305-331.

3. T. Causey-Bush, "Keep Your Eye on Texas and California: A Look at Testing, School Reform, No Child Left Behind and Implications for Students of Color," *Journal of Negro Education* 74,4 (2005): 332-343; and D. Hursh, "The Growth of High-Stakes Testing in the USA," 605-622.

4. C. Ascher, "Supplemental Education Services: Is This What our Students Need?" *Phi Delta Kappan* 88, 2 (2006): 136-141; J. Bathon and T. Spradlin, "Outcomes of the School

Choice and Supplemental Educational Services Provisions of NCLB." Education Policy Brief 5,8, Center for Evaluation and Education Policy, Indiana University, 2007; L.M. Anderson and K. Laguardia, *Case Studies of Supplemental Education Services Under the No Child Left Behind Act,* Washington, D.C.: U.S. Department of Education, 2005; and J. Kim and G.L. Sunderman, *Does NCLB Provide Good Choices for Students in Low-Performing Schools?* Cambridge, MA: Civil Rights Project at Harvard University, 2004.

5. Ibid.

6. E. Ayala, "Controversial 'Bump' in School Ratings Will Be Dropped," *(Ft. Worth) Star-Telegram,* April 22, 2011, accessed May 6, 2011, http://www.star-telegram.com/2011/04/22/3021036/controversial-bump-in-school-ratings.html; E. Mellon, "School Ratings at Risk," *Houston Chronicle,* April 22, 2011, accessed May 6, 2011, http://www.chron.com/disp/story.mpl/metropolitan/7533747.html; Texas Education Agency, *Accountability System for 2011- Standard Procedures, Commissioner of Education Final Decisions,* Austin, Tex., 2011; and B. Thevenot, "Projecting Success of Failing Students Often Wrong," *The Texas Tribune,* July 9, 2010, accessed December 3, 2010, www.texastribune.org.

7. Ayala, "Controversial 'Bump' in School Ratings"; Mellon, "School Ratings at Risk"; and Texas Education Agency, *Accountability System.*

8. Fusarelli, "The Potential Impact of the No Child Left Behind Act," 72-94.

9. Ibid.; and R.F. Elmore and S.H. Fuhrman, "Holding Schools Accountable: Is it Working?" *Phi Delta Kappan* 83,1 (2001): 67-72.

10. McDermott, "Expanding the Moral Community or Blaming the Victim?" 702-709; Hursh, "The Growth of High-Stakes Testing in the USA," 605-622; and Fusarelli, "The Potential Impact of the No Child Left Behind Act," 72-94.

11. Causey-Bush, "Keep Your Eye on Texas and California," 332-343.

12. Lee, "Is Test-Driven External Accountability Effective?" 608-644.

13. Hanushek and Raymond, "The Effect of School Accountability Systems on the Level and Distribution of Student Achievement," 406-415; Carnoy and Loeb, "Does External Accountability Affect Student Outcomes?" 305-331; E.J. Fuller and J. Johnson, "Can State Accountability Systems Drive Improvements in School Performance for Children of Color and Children From Low-Income Homes?" *Education and Urban Society* 33,3 (2001): 260-283; and J.J. Scheurich, L. Skrla, and J.S. Johnson. "Thinking Carefully About Equity and Accountability," *Phi Delta Kappan* (2000): 293-299.

14. Causey-Bush, "Keep Your Eye on Texas and California," 332-343; J. Booher-Jennings, "Below the Bubble: 'Educational Triage' and the Texas Accountability System," *American Educational Research Journal* 42,2 (2005): 231-268; Hursh, "The Growth of High-Stakes Testing in the USA," 605-622; H. Mintrop and G.L. Sunderman, "Predictable Failure of Federal Sanctions-Driven Accountability for School Improvement: And Why We May Retain it Anyway," *Educational Researcher* 38,5 (2009): 353-364; J. Lee and K.K. Wong, "The Impact of Accountability on Racial and Socioeconomic Equity: Considering Both School Resources and Achievement Outcomes," *American Education Research Journal* 41,4 (2004): 797-832.

15 Lee, "Is Test-Driven External Accountability Effective?" 608-644; Hanushek and Raymond, "The Effect of School Accountability Systems on the Level and Distribution of Student Achievement," 406-415.

16. Kim and Sunderman. "Measuring Academic Proficiency Under the No Child Left Behind Act," 3-13.

17. Bathon, J., and T. Spradlin. "Outcomes of the School Choice and Supplemental Educational Services Provisions of NCLB"; Mintrop and Sunderman. "Predictable Failure of Federal Sanctions-Driven Accountability for School Improvement," 353-364; Kim and Sunderman. "Measuring Academic Proficiency Under the No Child Left Behind Act," 3-13; Lee and Wong, "The Impact of Accountability on Racial and Socioeconomic Equity," 797-832; J.K. Rice and B. Malen, "The Human Costs of Education Reform: The Case of School Reconstitution," *Educational Administration Quarterly* 39,5 (2003): 635-666; B. Malen, R. Croninger, D. Muncey, and D. Redmond-Jones, "Reconstituting Schools: Testing the Theory of Action," *Educational Evaluation and Policy Analysis* 24,2 (2002): 113-32; G.D. Borman, L. Rachuba, A. Datnow, M. Alberg, M. Mac Iver, S. Stringfield, and S. Ross, "Four Models of School Improvement: Successes and Challenges in Reforming Low Performing, High Poverty Title I Schools," *Center for Research on the Education of Children Placed at Risk* 48 (2000): 2-81.

18. Accountability requirements change from year to year but are always based on three indicators: TAKS tests, completion rates, and dropout rates. In each of these categories a school must meet a certain requirement for all students as well as any subpopulation of minority for disadvantaged students if there are over 30 of them on the campus. Schools are rated as either Unacceptable, Acceptable, Recognized, or Exemplary. Unacceptable schools are subject to certain sanctions depending on the number of years they have been labeled as Unacceptable. These sanctions vary from providing outside tutoring to offering school choice to the largest sanction of school reconstitution. Actual sanctioning practices for each campus vary and are left largely to the discretion of the Commissioner of Education at the Texas Education Agency.

19. Texas Education Agency, *2009 Accountability Rating Manual,* Austin, Tex., 2009.

20. Texas Education Agency, *Texas Projection Measures (TPM): Questions and Answers,* Austin, Tex., 2010.

21. Ibid.

22. While tests scores are not the only measure used in accountability ratings, they are the only measure that utilizes TPM and is thus included in the analysis.

23. Ayala, "Controversial 'Bump' in School Ratings Will Be Dropped", Mellon, "School Ratings at Risk"; Texas Education Agency, *Accountability System for 2011-Standard Procedures, Commissioner of Education Final Decisions.*

24. United States Department of Education, *A Blueprint for Reform: The Reauthorization of the Elementary and Secondary Schools Act,* Washington, D.C., 2010, accessed May 6, 2011, http://www2.ed.gov/policy/elsec/leg/blueprint/index.html.

BIBLIOGRAPHY

Anderson, L.M., and K. Laguardia. *Case Studies of Supplemental Education Services Under the No Child Left Behind Act.* Washington, D.C.: U.S. Department of Education, 2005.

Ascher, C. "Supplemental Education Services: Is This What our Students Need?" *Phi Delta Kappan, 88, 2 (2006):* 136-141.

Ayala, E. "Controversial 'Bump' in School Ratings Will Be Dropped," *Star-Telegram, April 22, 2011.* Accessed May 6, 2011, http://www.star-telegram.com/2011/04/22/3021036/controversial-bump-in-school-ratings.html.

Bathon, J., and T. Spradlin. "Outcomes of the School Choice and Supplemental Educational Services Provisions of NCLB." Education Policy Brief 5,8. Center for Evaluation and Education Policy, Indiana University, 2007.

Booher-Jennings, J. "Below the Bubble: 'Educational Triage' and the Texas Accountability System." *American Educational Research Journal 42,2* (2005): 231-268.

Borman, G.D., L. Rachuba, A. Datnow, M. Alberg, M. Mac Iver, S. Stringfield, and S. Ross. "Four Models of School Improvement: Successes and Challenges in Reforming Low Performing, High Poverty Title I Schools," *Center for Research on the Education of Children Placed at Risk* 48 (2000): 2-81.

Carnoy, M., and S. Loeb. "Does External Accountability Affect Student Outcomes? A Cross-State Analysis." *Educational Evaluation and Policy Analysis* 24,4 (2002): 305-331.

Causey-Bush, T. "Keep Your Eye on Texas and California: A Look at Testing, School Reform, No Child Left Behind and Implications for Students of Color." *Journal of Negro Education* 74,4 (2005): 332-343.

Elmore, R.F., and S.H. Fuhrman. "Holding Schools Accountable: Is it Working?" *Phi Delta Kappan* 83,1 (2001): 67-72.

Fuller, E.J., and J. Johnson. "Can State Accountability Systems Drive Improvements in School Performance for Children of Color and Children From Low-Income Homes?" *Education and Urban Society* 33,3 (2001): 260-283.

Fusarelli, L.D. "The Potential Impact of the No Child Left Behind Act on Equity and Diversity in American Education." *Educational Policy* 18,71 (2004): 72-94.

Hanushek, E.A., and M.E. Raymond. "The Effect of School Accountability Systems on the Level and Distribution of Student Achievement." *Journal of the European Economic Association* 2,2/3 (2004): 406-415.

Hursh, D. "The Growth of High-Stakes Testing in the USA: Accountability, Markets and the Decline in Educational Inequality." *British Educational Research Journal* 31,5 (2005): 605-622.

Kim, J., and G.L. Sunderman. *Does NCLB Provide Good Choices for Students in Low-Performing Schools?* Cambridge, MA: Civil Rights Project at Harvard University, 2004.

Kim, J.S., and G.L. Sunderman. "Measuring Academic Proficiency Under the No Child Left Behind Act: Implications for Educational Equity." *Educational Researcher* 34,8 (2005): 3-13.

Lee, J. "Is Test-Driven External Accountability Effective? Synthesizing the Evidence From Cross-State Causal-Comparative and Correlational Studies." *Review of Educational Research* 78,3 (2008): 608-644.

Lee, J., and K.K. Wong. "The Impact of Accountability on Racial and Socioeconomic Equity: Considering Both School Resources and Achievement Outcomes." *American Education Research Journal* 41,4 (2004): 797-832.

Malen, B., R. Croninger, D. Muncey, and D. Redmond-Jones. "Reconstituting Schools: Testing the Theory of Action." *Educational Evaluation and Policy Analysis* 24,2 (2002): 113-32.

McDermott, K.A. "Expanding the Moral Community or Blaming the Victim? The Politics of State Education Accountability Policy." *American Education Research Journal* 44,1 (2007): 702-709.

Mellon, E. "School Ratings at Risk." *Houston Chronicle, April 22, 2011.* Accessed May 6, 2011, http://www.chron.com/disp/story.mpl/metropolitan/7533747.html.

Mintrop, H., and G.L. Sunderman. "Predictable Failure of Federal Sanctions-Driven Accountability for School Improvement: And Why We May Retain it Anyway." *Educational Researcher* 38,5 (2009): 353-364.

Rice, J. K., and B. Malen. "The Human Costs of Education Reform: The Case of School Reconstitution." *Educational Administration Quarterly* 39,5 (2003): 635-666.

Scheurich, J.J., L. Skrla, and J.S. Johnson. "Thinking Carefully About Equity and Accountability." *Phi Delta Kappan* (2000): 293-299.

Texas Education Agency. *2009 Accountability Rating Manual.* Austin, Tex. 2009.

Texas Education Agency. *Texas Projection Measures (TPM): Questions and Answers.* Austin, Tex. 2010.

Texas Education Agency. *Accountability System for 2011- Standard Procedures, Commissioner of Education Final Decisions.* Austin, Tex. 2011.

Thevenot, B. "Projecting Success of Failing Students Often Wrong." *The Texas Tribune.* July 9, 2010. Accessed December 3, 2010, http://www.texastribune.org

United States Department of Education. *A Blueprint for Reform: The Reauthorization of the Elementary and Secondary Schools Act.* Washington, D.C. 2010. Accessed May 6, 2011, http://www2.ed.gov/policy/elsec/leg/blueprint/index.html.

Cyber Warfare:
The Frontline of 21st Century Conflict

Marc Olivier, mgolivier@hotmail.com
LBJ School of Public Affairs

The United States is increasingly dependent on cyberspace to carry out everyday functions. While cyberspace is often viewed as a virtual world, it is composed of vulnerable physical infrastructure. The vast amount of digital infrastructure that supports the Internet, the economy, the government, and the military makes it nearly impossible to guarantee total security. The more dependent a country becomes on the Internet and the more interconnected its systems become, the more vulnerable the country is to hackers or foreign intelligence services conducting espionage. The National Intelligence Council stated in its most recent quadrennial report, *Global Trends 2025: A Transformed World,* that the increasing use of cyber warfare is one of the primary factors that "will constrict U.S. freedom of action."[1] It is particularly difficult for the U.S. government to respond to cyber attacks because it is very difficult to track the source of an attack and to determine who initiated it. The international race to build cyber defenses and to develop offensive capabilities, as well as the lack of law governing cyberspace, makes cyber warfare one of the most urgent national security problems facing the United States.

Cyberspace is a Real and Growing Threat

Cyberspace is wrongly viewed as something that cannot be seen, only existing in a virtual form. Cyberspace is real and has very physical components. It exists in the computer systems that enable Wall Street to function and it forms the backbone of all major companies. Cyberspace also exists in the critical infrastructure that allows computers to communicate with each other, such as the main communication trunk line from Europe to the United States that comes up on the New Jersey shore. It plays a major role in the functioning of software, computers, and

cell phones, all of which are now common in daily life. Cyberspace includes the broadband networks, wireless signals, and local area networks in schools. It also encompasses the critical military and intelligence networks designed to protect the United States. While the Internet has made society more interconnected than at any time in history, it has also made it easier for domestic and foreign hackers to disrupt daily life.

Cyber attack refers to a deliberate action to "alter, disrupt, deceive, degrade, or destroy" networks, computer systems, or programs that may be contained on a computer or moving through a system.[2] A cyber attack generally involves penetrating a computer network as a means to disrupt an opponent's critical services, such as accessing a utility control system. Groups that operate independently or with state sponsorship that can gain access to intellectual property or classified military information are a growing threat. However, there are legitimate uses of cyber attacks. The United States prepares to conduct cyber attacks in conjunction with other information warfare methods and with conventional attacks to protect national security. Domestic law enforcement also engages in cyber attacks when jamming devices are used to prevent cell phone calls when suspected to be used to detonate a bomb.

Cyber attacks became much more common during the late 1990s, including such cases as the 1998 Internet Worm, Melissa Virus, I-LOVE-YOU virus, Code Red Virus, and the Nimda Virus. Initially, attacks consisted of malware, such as viruses and worms. Today, cyber attacks are increasingly sophisticated and adaptive. Security breaches and information theft are commonplace in the news. Foreign intelligence services from countries such as China, Israel, Iran, Russia, and the United States have used cyber capabilities defensively and offensively.

The first major test of the U.S. government's cyber infrastructure from cyber attacks was Eligible Receiver in June 1997, a Joint Staff test exercise run by the Department of Defense (DOD).[3] The unannounced exercise targeted 20 different agencies and revealed significant vulnerabilities within the U.S. government's information infrastructures. A team of 35 computer experts from the National Security Agency split into four teams to simulate hackers trying to penetrate U.S. computer networks. The teams used publicly available information and tools found on the Internet and commercial Internet accounts to exploit actual vulnerabilities. Over the next two weeks they successfully hacked into power grids of nine U.S. cities and cracked their 911 emergency systems. They also attacked the Pentagon's computer networks, gaining access to 36 of them. Only two of the attacks were detected. Once inside the systems, the teams had complete access and were able to issue fake orders and news reports about the crisis. As a result, no one in the entire chain of command could be certain of what was accurate. If it had been a real attack, the four teams would have been able to prevent the United States from responding effectively.[4]

The severity of security challenges posed by cyber warfare to any country is highly related to the degree of its dependence on modern information and communications technology. Countries with advanced internet accessibility, including widespread online commerce and banking, possess far more vulnerabilities to at-

tack. Countries with limited reliance on information technology (IT) are much less exposed, but still susceptible to cyber attacks. For example, an undercover Defense Department employee said that it would be possible to hit three undisclosed communication "nodes" in the United States and severely impair communications across the country.[5] The Department of Energy conducted an experiment, the Aurora Generator Test, to determine if a 27-ton power generator could be disabled using the Internet.[6] The group of scientists was able to hack into the control system and use the controls to cause the generator to shudder, overheat, and eventually to fatally malfunction. In a real world scenario, losing several large power generators would cause a prolonged disruption. The generators are expensive, made overseas, and require up to four months to obtain. A well-targeted cyber attack could shut down a power plant for months.[7] The power grid is one of the most vulnerable infrastructure systems to cyber attack in part because it is operated by private utilities that are not required to comply with government security decrees.[8] With the move toward a Smart Grid, which relies on interconnected networks of computer-controlled nodes, its vulnerability could increase because each node would operate automatically over the Internet to regulate the flow of power. If the nodes are not secure, they can be hacked and used to disrupt the delivery of electricity.[9] Additionally, there are only about five software systems used to run power grids, dams, utilities, and pipelines that rely on wireless supervisory control and data acquisition (SCADA) systems in which one node provides instructions to another node in the chain. If compromised, the SCADA system could send fake instructions, potentially causing severe damage to critical infrastructure. One of the benefits of the outdated air traffic control system in the U.S. is that because it is so old, it is not directly connected to the Internet, and is less susceptible to a cyber attack.[10]

Every day there are thousands of cyber attacks on federal and private computer systems. The DOD estimated that in 2007 there were 43,880 incidents of malicious activity from all sources on five million computers, a 31 percent increase from 2006.[11] Some attacks are malicious, but others appear to be testing the chinks in the patchwork of firewalls. The most dangerous aspect is the attacks that go undetected by common security tools. The number of attacks is increasing and they are becoming increasingly bold. In January 2008, a Central Intelligence Agency (CIA) official stated that the CIA knew hackers had disrupted or threatened to disrupt power in four foreign cities.[12] The enormous challenge of defending cyber infrastructure ranges from forensic tasks to determine attack attribution to the broader concern of proportionality of a response and what is considered a legitimate target.

A CSIS panel researched potential vulnerabilities and determined that the main threat is not the capabilities of individual hackers but the capabilities of other nations, such as China and Russia. Team Cymru, a research company, reviewed Internet scans that attempted to enter industrial control systems. Scans originated from 14 different countries, including China, Iran, Israel, Russia, Taiwan, and even the United States. The Team Cymru results showed that 90 percent of the scans originated in China.[13]

Although scanning alone does not cause any damage to computer systems, it could be a preliminary step in an actual attack that would scramble databases or control computers. Former Director of National Intelligence (DNI) Mike McConnell told President Bush in 2007 that if a large U.S. bank were successfully hacked, "it would have an order-of-magnitude greater impact on the global economy" than the September 11, 2001, attacks. McConnell warned, "the ability to threaten the U.S. money supply is the equivalent of today's nuclear weapon."[14] A cyber attack on the banking system could shut down the system that clears all financial transactions, thus undermining all confidence in the monetary system.

In a cyber war, it is difficult to determine the source of an attack or the attacker's identity. The ability to backtrack a cyber attack to the source depends on a rapid response capability on the order of seconds, minutes, or hours. The pathways used by hackers may only be active for milliseconds and often there is no identifying evidence that remains once the hacker has completed his objective. In the case of the Team Cymru study, the team could not identify whether military organizations, intelligence agencies, terrorists, criminals, or inventive individuals were the source of the cyber attacks.[15] Even if the physical origin of an attack can be identified, there is no guarantee that the hacker behind the attack is sponsored by that country or that the hacker is even located within the given country.[16]

A new type of cyber warfare that is growing is hybrid warfare.[17] National governments rather than individual hackers carry out this type of attack. Hybrid warfare is a cyber attack that is timed to coincide with a conventional military offensive. A cyber attack using mass communication sources in conjunction with a conventional military attack may also be used to influence global public opinion.[18] Hybrid warfare is particularly threatening because it is designed to prevent an effective response by the targeted country to a physical attack.

An offensive tool in the cyber arsenal is the botnet, a collection of computers that have been compromised by malicious software. The program commandeers the infected machines, creating a vast network. The compromised computers, known as "zombies," can be remotely controlled, often without the knowledge of anyone using the zombie computer. The zombie network can be instructed to attack a designated target by overwhelming it with thousands of commands.[19] In an actual cyber war, a successful cyber attack would target computer-dependent infrastructure, such as a nation's power grid or banking system. Also, an attack on a nation's air traffic control system could blind the air traffic controllers' air defense networks, hindering an effective counterstrike.[20]

USE OF CYBER WARFARE BY FOREIGN INTELLIGENCE SERVICES

CYBER ATTACK ON ESTONIA

In 2007, Estonia was subject to a prolonged cyber attack suspected of being sponsored by Russia. Estonia, a developed former Soviet Republic, has a high level of access to advanced communications technology. The Estonian government shifted all of its major government operations to the Internet in 2005. The government

holds all cabinet meetings online and documents are signed with e-signatures. Beginning in March 2007, Estonians can even vote online.[21] Over 60 percent of the population has online access to bank accounts and 95 percent of banking transactions are online.[22] Russian hackers were patiently waiting for a pretext to test Estonia's cyber defenses.

In April 2007, the Estonian government decided to relocate a monument that commemorated the Soviet armed forces' contribution to liberating Estonia from Nazi control during World War II. Moving the monument from the center of Tallinn, the capital, to a military cemetery outside the city sparked protests and riots among the Russian minority. The event may have provided the pretext, and the unrest was closely followed by distributed denial of service (DDOS) attacks originating in Russia.[23] A call to action and step-by-step instructions about how to carry out DDOS attacks spread through Russian chat rooms. The Estonian government websites that normally received 1,000 visitors per day suddenly started receiving 2,000 visits per second.[24] Anyone who attempted to access the target sites had their computer screens frozen.[25] The websites of the Ministry of Foreign Affairs and the Ministry of Justice shut down, and the Prime Minister Andrus Ansip's Reform Party website was defaced by the addition of an image of Prime Minister Ansip with an Adolf Hitler mustache. The Russian hackers also briefly disabled the national emergency phone number.[26]

The United States and NATO sent computer security teams to aid the Estonian authorities to cope with the DDOS waves that overpowered the country's government websites, banking industry, and media organizations. The clandestine groups of hackers were not confirmed to be operating with Russian sponsorship, but evidence suggests the Russian authorities were at least complicit.[27] The unusual aspect of the attacks was that they lasted for several weeks and had a very high intensity. Some of the botnets used in the DDOS attacks included up to 100,000 zombie computers. The commandeered computers directed large amounts of data at Estonia's government websites and banking system.[28] The US-NATO efforts stabilized the situation, but intermittent attacks continued until mid-May 2007.[29]

In response to the cyber attacks, NATO established the Cooperative Defense Center in Estonia in May 2008. The center is staffed by 30 cyber specialists and is part of NATO's network of Centers of Excellence accredited to train representatives from member states about technical aspects of NATO operations.[30] However, the new center's vulnerability was shown with the capture of Herman Simm in September 2008, which also further implicated Russia in the cyber attack on Estonia.[31]

Herman Simm, 61, was a high ranking official working in the Estonian Ministry of Defense. In 2001, he was appointed head of the State Secret Protection Office. He also developed the information protection systems for NATO and the European Union, frequently leading Estonian talks on protecting classified data. He was described as being "at the cutting edge of NATO's most important new strategic missions: to defend the alliance against cyber-attack."[32]

Recruited as an asset by Russia in the late 1980s, he was accused of providing classified U.S. missile shield and cyber defense information to the Russian Foreign Intelligence Service for millions of dollars. The Estonian government issued Simm

a diplomatic passport that he used to personally transfer documents abroad.[33] Although it is unknown if he had other accomplices within the government, Simm oversaw the issuance of security clearances for Estonian intelligence, military, and security agencies.[34] An Estonian court convicted Simm of treason in February 2009. He was ordered to pay $1.6 million and sentenced to 12 years in prison for damage to security systems.[35]

In November 2008, the United States DOD computers were subject to a retaliatory cyber attack thought to originate in Russia.[36] The attack spread throughout the computer network via agent.btz malware, which was designed specifically to target military computers. The malware damaged computer networks in U.S. Central Command, including computers used in Iraq and Afghanistan. The attack also penetrated another highly classified DOD network.[37] The Pentagon banned all use of flash drives, which was believed to be the method of delivering the malware to the computer network. Several intelligence sources say evidence indicates Russian government involvement, which if correct, would make it the first time a major cyber power successfully invaded classified U.S. military networks.[38]

In April 2009, NATO expelled two Russians. One was the son of Vladimir Chizhov, the Russian ambassador to the European Union.[39] He and the other diplomat were assigned to Russia's mission to NATO and were suspected of working undercover as spies. The computer systems of NATO and the DOD have since been upgraded with "enhanced security measures."[40]

RUSSIA-GEORGIA WAR

The Russia-Georgia War of 2008 may be the first instance of the use of hybrid warfare in which a cyber attack preceded a conventional military strike. Despite the Russian government's denial of involvement in the cyber attack, the planning, servers of Russian state-owned businesses, and timing of the attack suggest some degree of coordination or direction by the Russian government.[41] The cyber attack began with a series of small-scale DDOS attacks in June 2008, two months prior to the five-day war over the breakaway region of South Ossetia.[42] The cyber attacks made use of botnets, which loaded computers with malicious software. The hackers then ordered the zombie computers to send millions of requests to designated websites to overwhelm the server causing it to shut down. On July 20, several DDOS attacks on President Mikhail Saakashvili's official website caused it to shut down for over 24 hours.[43] Reports indicated that the cyber attack came from a "command-and-control server" set up several weeks earlier in the United States, which shows that planning and coordination are not confined to national borders.[44] The U.S.-based server became operational many weeks ahead of the actual attacks, and by August 8, the first day of the war, the rate of cyber attacks had escalated to a very high level. Six botnets launched a coordinated cyber attack on Georgian government and media websites.[45] The cyber attacks also increased in intensity along with the physical conflict between Russian and Georgian troops. The websites of the President, Parliament, Ministry of Defense, Ministry of Foreign Affairs, the National Bank of Georgia, and the online news agencies of The Messenger and Civil.ge all shut down. The websites of the Ministry of Foreign Affairs and the

National Bank were defaced by adding images comparing Saakashvili with Adolf Hitler.[46] Although defacing a government website has a visual impact, shutting down online media sources during a military attack is characteristic of information warfare with the intent to disrupt communication and prevent dissemination of accurate information.

The Georgian government reacted by requesting permission from Google to transfer the websites of the Ministry of Foreign Affairs and Civil.ge to the Blogspot domain, which were better protected from the DDOS attacks.[47] Atlanta-based Tulip Systems, Inc. agreed to host the President's website. Polish President Lech Kacyznski provided space on his website for official Georgian press releases, and Estonia hosted the Ministry of Foreign Affairs and sent two information security specialists to support Georgian cyber defenses.[48]

Reports indicated that StopGeorgia.ru, which was established within hours of Russian forces entering South Ossetia, was a main coordinator of the cyber attacks.[49] The forum provided a continuously updated list of target websites. It also encouraged visitors to download DoSHTTP, a free software program, to allow them to participate in the DDOS attacks.[50]

Project Grey Goose, an independent project launched by cyber specialist Jeff Carr and 100 computer security, technology, and intelligence volunteers, attempted to determine the source of the cyber attacks. Although, the group was unable to verify Russian-sponsorship of StopGeorgia.ru and another website, Xakep.ru, it is still reasonable to conclude a link exists. Russian government members clearly supported the sites' efforts and their implied consent by refusing to take action against the sites to stop the cyber attacks.[51] Project Grey Goose also found that the hackers made extensive use of SQL attacks, which are simpler than DDOS attacks. The SQL attacks exploit vulnerabilities within MySQL, a popular open source software which websites commonly use to manage databases. The targeted database is overwhelmed with millions of extraneous queries, shutting down the server. The benefit of using a combined SQL and DDOS attack is that it is very difficult to detect.[52] SQL attacks also do not require as many computers to have the same impact as a DDOS attack that cannot be kept up without botnets. The methods used showed "planning, organization, targeted reconnaissance, and evolution of attacks."[53]

The cyber attacks on Georgia in 2008 did not cause nearly the damage that they did in Estonia in 2007 because Georgia's economy and infrastructure are not fully integrated to the Internet—only 7 percent of the country has access to the Internet, with only limited coverage outside Tiblisi.[54] Nevertheless, the attacks disrupted timely dissemination of information by the Georgian government and forced it to seek alternative methods for distributing information to the international community.

China and Cyber Attacks

China is a main threat to cyber security because of the large number of Internet users and because of the high number of attacks originating in the country that are more sophisticated than other actors.[55] China also regards cyber warfare as

a central component in future conflicts, such as with the United States, where a direct confrontation would be difficult.[56] This is an example of asymmetric warfare, where one actor, a country or non-state entity, undermines another country's strength by exploiting its weaknesses.[57] Asymmetric conflict involves a tactical operation whose objective is to prevent the opponent from engaging in battle. This vision makes sense from China's perspective because it must counter the United States' technological advantage. Cyber attacks from China are not new. China launched cyber attacks in response to U.S. planes bombing the Chinese embassy in Belgrade, and following the crash of a Chinese fighter after it collided with a U.S. surveillance plane. In 2002, U.S. government servers were the target of coordinated cyber attacks, code-named Titan Rain, which originated in China.[58] Targeted locations included the U.S. Army Information Systems Engineering Command, the Naval Ocean Systems Center, the Missile Defense Agency, and Sandia National Laboratories. China downloaded between 10 and 20 terabytes of data, or roughly the amount of information contained in the entire Library of Congress. The cyber attacks sought to gain information about military and government activities. China also conducted reconnaissance of the U.S. command and control system, information that it could use in future cyber attacks.[59]

In addition to the United States, China has targeted other Western nations. The German Vice President of the Office for the Protection of the Constitution, Hans Elmar Remberg, accused China of carrying out computer network intrusions on an "almost daily" basis.[60] French Secretary-General of National Defense Francis Delon confirmed that the Chinese had targeted many French government websites in September 2007.[61] In November 2007, MI-5 Director Jonathan Evans warned financial service companies that they were the targets of "state-sponsored computer network exploitation."[62] In the cyber attacks on the British financial system, the Chinese hackers were suspected of successfully obtaining strategic plans and risk management systems of Lehman brothers, Britain's Bradford & Bingley, and Iceland's Landsbanki.[63]

Chinese hackers associated with the People's Liberation Army (PLA) carried out an attack on Pentagon computer networks that lasted for several weeks in 2007.[64] The cyber attacks overpowered the defenses mounted by U.S. military computer experts. The cyber attacks overpowered the defenses mounted by U.S. military computer experts. The Chinese hackers gained accessed to the unclassified computer system that supports the Secretary of Defense. To avoid further damage, the Pentagon shut down the network. [65] The cyber attack resulted in the creation of the National Cyber Investigative Joint Task Force to "coordinate, integrate, and share information related to all domestic cyber threat investigations."[66]

By 2005, the Chinese PLA had formed "information warfare militia units" charged with developing viruses to attack enemy computer systems and networks.[67] There are thought to be about 250 hacker groups in China that are either tolerated or encouraged by the government.[68] One such group was the Network Crack Program Hacker (NCPH) that had ties to the PLA. NCPH developed software that allowed remote control of network programs, enabling the organization to steal government documents. NCPH also took advantage of holes in Microsoft Of-

fice to insert Trojans that took partial control of the computers to extract files. In 2006, NCPH began using these programs to steal millions of unclassified U.S. government documents.[69] NCPH consisted of eight people in their early 20s who attended Sichuan University. The group first started hacking websites in China, eventually coming to the attention of the Sichuan Military Command Communication Department, which instructed them to participate in a cyber attack network training. After winning the provincial military command competition, the NCPH members entered advanced training consisting of simulated attacks, designing hacking tools, and drafting network-infiltration techniques. Eventually, the NCPH gained a benefactor, likely the PLA, which began subsidizing the group at $270 dollars per month.[70]

China is interested in aggressively acquiring commercial secrets and information on future weapons systems.[71] The closed and authoritarian nature of the Chinese state and its tight regulation of the Internet make it tough to imagine large hacker communities operating freely without state supervision. The lack of transparency regarding Chinese military modernization and yearly increases in military expenditures is a main concern for the Pentagon. Chinese use of cyber warfare is becoming increasingly sophisticated. Although, the Chinese space program is focused mostly on civilian uses, it is providing the PLA with the ability to track U.S. forces in the western Pacific Ocean. China's advances in cyber technology will jeopardize the U.S. military communication systems that depend on wireless communications and computer networks.[72] In addition, China is targeting defense contractors, such as Raytheon, Lockheed Martin, Boeing, and Northrop Grumman, all of which have had their unclassified networks penetrated by Chinese hackers. In 2005, Chinese hackers were able to obtain the Army's and Air Force's flight planning software from Redstone Arsenal, Alabama.[73] Furthermore, Chinese operations have been detected inside certain U.S. electricity grids. The Chinese have the capability to map electric networks and leave behind malicious software to sabotage networks later. Former DNI McConnell stated he would be surprised if tools and capabilities have not been left in computer and information systems that could be put into action at some time in the future.[74]

Current waves of cyber attacks from China are aimed mainly at collecting information and probing defenses. China is likely to continue to exploit U.S. dependence on cyberspace because of low operations costs compared to traditional espionage methods or military activities. Cyber attacks create confusion, and there is no legal framework for cyber warfare.[75] An international legal framework provides a basis for deterring cyber attacks by creating a cost and international pressure for violating an accepted norm.[76]

A Cyber Arms Race

The cyber attacks being detected today and the use of hybrid warfare in the Russia-Georgia War are the beginning of a new international race to develop cyber weapons and the defenses to protect against them. As the Internet spreads to ever more distant parts of the world, and national economies become increasingly

integrated into the World Wide Web, the desire to acquire both offensive and defensive cyber capabilities by states and non-state actors will multiply. China is an advanced technology products exporting power and a leader in the semiconductor industry, which gives it unique access to technology components.[77] This access also provides a potential opening for launching cyber attacks.[78]

If an imminent attack was detected, some officials argue that the United States should pre-emptively strike the source, ranging from an online attack to a physical strike, as a means to deter future cyber attacks.[79] Other officials argue that pre-emptive attacks would provide justification for foreign governments to invest in their own efforts to engage in cyber warfare and to pre-emptively attack the United States.[80] With the numbers of hackers and the superior computing ability that comes from harnessing tens of thousands of computers around the world in botnets, someone will find a way to breach a network security system. In the long run, it is not possible to simply build more advanced cyber defenses. The best defense against a cyber attack is to develop a robust capability to engage in cyber war and develop the necessary defenses to mitigate a cyber attack.

The benefit of Eligible Receiver in the early days of cyber attacks is that federal agencies, research groups, and military contractors now frequently run war games to assess U.S. vulnerabilities. Although President Obama has not spoken openly about whether he supports or opposes cyber weapons, it would be irresponsible not to develop them to protect against attacks. These capabilities are also critical because they can provide vital intelligence, and foreign intelligence services are already using such capabilities, or investing heavily in developing them. U.S. intelligence agencies could activate code embedded in computer chips during the manufacturing process that would enable the U.S. to remotely control an enemy's computers over the Internet. However, the U.S. potentially runs the same risk from computer chips made in China.

Currently, there is no broad authorization for American forces to engage in cyber war. Former President Bush attempted to include a section to improve U.S. cyber defenses in a classified set of presidential orders in January 2008, but the administration failed to agree on how to write the authorization.[81] Instead, President Bush authorized individual uses of cyber warfare in Iraq and Iran.[82]

In 2003, the Pentagon and U.S. intelligence agencies made plans for a cyber attack on Saddam Hussein's bank accounts. The plan would have frozen billions of dollars and crippled the Iraqi government's financial system in advance of the U.S. invasion of Iraq. Saddam Hussein would have had no money for war supplies or money to pay troops.[83] Bush administration officials were concerned that the plan might not be limited to Iraq, potentially causing global financial disorder, spreading throughout the Middle East to Europe, and to the United States. Therefore, the plan was never carried out. However, President Bush did approve a plan to disable Iraq's military and government communications.[84] The U.S. government contacted international communications companies that provided satellite and cell phone coverage in Iraq to warn them about jamming and to request support by turning off their signals. The communications jamming did affect surrounding countries that shared communication systems with Iraq, but the damage was considered

acceptable by the Bush administration. Another cyber attack allowed the U.S. to hack into an Al Qaeda computer and alter information to lead an Al Qaeda group to where U.S. forces were waiting. President Bush also approved an experimental program that would allow the U.S. to slow Iran's progress towards production of a nuclear bomb.[85]

DISCUSSION

President Obama expanded a $17 billion, five-year program, known as the Comprehensive National Cybersecurity Initiative, authorized by President Bush in 2008.[86] In December 2009, President Obama appointed Howard Schmidt to fill the White House cyber security coordinator, after Melissa Hathaway resigned in August 2009, citing delays in the appointment process.[87] Secretary Robert Gates approved the creation of the U.S. Cyber Command (USCYBERCOMM) headed by the director of the National Security Agency, to be the nation's central hub for cyber capabilities. USCYBERCOMM incorporates the Joint Task Force-Global Network Operations (JTF-GNO) and the Joint Functional Component Command-Network Warfare (JFCC-NW). The organization will build the defenses for military computers and communications systems as well as developing and deploying cyber weapons.[88] The Pentagon has already commissioned military contractors to develop a classified version of the future Internet, known as the National Cyber Range, on which to test simulated cyber attacks to improve U.S. defenses.[89]

It is clear the rapid dissemination of information and technology will only magnify the threat of cyber warfare in years to come. The Russian-based attacks on Estonia and Georgia showed how cyber attacks defy state borders and raise difficult issues of jurisdiction. It also shows Russia's preference of using cyber attacks to settle scores with former Soviet states. In addition, China is exhibiting a keen interest in industrial espionage and aggressive intelligence gathering through cyber attacks against Western governments. In April 2011, President Obama announced the National Strategy for Trusted Identities in Cyberspace as a means to increase trustworthiness of identities in online transactions in response to fraud and identity thefts.[90] The U.S. will have to spearhead the formation of a legal framework for this new challenge, complete with definition of vital terms and rules of the game. The main tenets of warfare embedded in the UN Geneva Conventions will have to be revised to incorporate cyber warfare because it blurs the principles of proportionality, neutrality, and distinction. Yet the most serious problem of cyber warfare is that countries do not know how good the weapons are until they are used.

ENDNOTES

1. National Intelligence Council, *Global Trends 2025: A Transformed World* (Washington, D.C.: U.S. Government Printing Office, 2008), xi, accessed November 16, 2009, http://www.dni.gov/nic/PDF_2025/2025_Global_Trends_Final_Report.pdf.

2. William A. Owens, Kenneth W. Dam, and Herbert S. Lin, *U.S. Acquisition and Use of Cyberattack Capabilities* (Washington, D.C.: National Academies Press, 2009), 1, accessed November 16, 2009, http://www.nap.edu/catalog.php?record_id=12651#toc/.

3. James F. Dunnigan, *The Next War Zone: Confronting the Global Threat of Cyberterrorism* (New York: Kensington Publishing Corporation, 2002): 68.

4. James Adams, "Virtual Defense," *Foreign Affairs* 80,3 (May-June 2001): 101.

5. *Frontline,* "Cyber War!" PBS, April 24, 2003, accessed November 16, 2009, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html.

6. Charles Ebinger and Kevin Massey, "Software and Hard Targets: Enhancing Smart Grid Cyber Security in the Age of Information Warfare," *Brookings Energy Security Initiative* (February 2011), 7, accessed May 7, 2011, http://www.brookings.edu/~/media/Files/rc/papers/2011/02_smart_grid_ebinger/02_smart_grid_ebinger.pdf.

7. *Frontline,* "Cyber War!" PBS, April 24, 2003, accessed November 16, 2009, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/.

8. 60 Minutes, "Cyber War: Sabotaging the System," CBS, November 8, 2009, accessed November 16, 2009, http://www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml.

9. James A. Lewis, "Cyber Security – Assessing Our Vulnerabilities and Developing an Effective Defense" (Statement, CSIS, Senate Committee on Commerce, Science, and Transportation, March 19, 2009), accessed November 16, 2009, http://www.csis.org/files/media/csis/congress/ts090319_lewis.pdf.

10. David E. Sanger, John Markoff, and Thom Shanker, "U.S. Steps Up Effort on Digital Defenses," *New York Times,* April 28, 2009, accessed November 16, 2009, http://www.nytimes.com/2009/04/28/us/28cyber.html.

11. U.S.-China Economic and Security Review Commission, *USSC 2008 Annual Report* (Washington, D.C.: U.S. Government Printing Office, 2008), 163, accessed November 16, 2009, http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf/.

12. Center for Strategic International Studies, "Significant Cyber Incidents Since 2006" (working paper, November 6, 2009), accessed November 16, 2009, http://www.csis.org/files/publication/100120_CyberEventsSince2006.pdf.

13. Sanger, Markoff, and Shanker, "U.S. Steps Up Effort on Digital Defenses."

14. Ibid.

15. Ibid.

16. *Frontline,* "Cyber War!" PBS, April 24, 2003, accessed November 16, 2009, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html/.

17. U.S. General Accountability Office, "Hybrid Warfare," GAO-10-1036R (September 10, 2010), 18.

18. Department of Defense, *National Defense Strategy* (June 2008), 4, accessed November 16, 2009, http://www.defenselink.mil/pubs/2008NationalDefenseStrategy.pdf.

19. OECD, "Malicious Software (Malware): A Security Threat to the Internet Economy." Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL (June 2008), 22, accessed May 7, 2011, http://www.oecd.org/dataoecd/53/34/40724457.pdf.

20. Sanger, Markoff, and Shanker, "U.S. Steps Up Effort on Digital Defenses."

21. Cyrus Farivar, "Cyberwar I: What the Attacks on Estonia Have Taught Us about Online Combat," *Slate,* May 22, 2007, accessed November 16, 2009, http://www.slate.com/id/2166749/.

22. Johnny Ryan, "iWar: A New Threat, Its Convenience, and Our Increasing Vulnerability," *NATO Review* (Winter 2007), accessed November 16, 2009, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html/.

23. U.S. Congressional Research Service, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress* (RL32114; January 29, 2008), by Clay Wilson, 7, accessed November 16, 2009, http://fas.org/sgp/crs/terror/RL32114.pdf/.

24. Ibid.

25. Sanger, Markoff, and Shanker, "U.S. Steps Up Effort on Digital Defenses."

26. Toomas Hendrik, interview, *Russia: Estonian President Says Moscow Sees Democracy as a 'Threat',* Radio Free Europe/Radio Liberty, June 5, 2007, accessed November 16, 2009, http://www.rferl.org/content/article/1076942.html/.

27. Ian Traynor, "Russia Accused of Unleashing Cyberwar to Disable Estonia," *The Guardian,* May 17, 2007, accessed November 16, 2009, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

28. Ryan, "iWar."

29. Farivar, "Cyberwar I."

30. Vladimir Socor, "NATO Creates Cyber Defense Center in Estonia," *Eurasia Daily Monitor,* May 15, 2008, accessed November 16, 2009, http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33636/.

31. Roger Boyes, "Russian Spy in NATO Could Have Passed on Missile Defense and Cyber-War Secrets," *Times Online,* November 16, 2009, accessed November 16, 2009, http://www.timesonline.co.uk/tol/news/world/europe/article5166227.ece.

32. Ibid.

33. Ibid.

34. Ibid.

35. Michael Schwirtz, "Former Estonian Official Convicted of Treason," *New York Times,* February 25, 2009, accessed November 16, 2009, http://www.nytimes.com/2009/02/26/world/europe/26estonia.html/.

36. Julian Barnes, "Cyber Attack Has Pentagon Worried," *Chicago Tribune,* November 30, 2008, accessed November 16, 2009, http://www.chicagotribune.com/news/nationworld/chi-cyberattack_bdnov30,0,633998.story/.

37. Ibid.

38. Rebecca Grant, "Cyber Menace," *Airforce Magazine,* March 2009, 24, accessed November 16, 2009, http://www.airforce-magazine.com/MagazineArchive/Pages/2009/March%202009/0309cyber.aspx.

39. Tony Barber, "NATO Expels Russian Envoys," *Financial Times,* April 29, 2009, accessed November 16, 2009, http://www.ft.com/cms/s/0/39446224-3500-11de-940a-00144feabdc0.html.

40. Julian Barnes, "Cyber Attack Has Pentagon Worried," *Chicago Tribune,* November 30, 2008, accessed November 16, 2009, http://articles.chicagotribune.com/2008-11-30/news/0811300082_1_military-networks-computers-flash-drives.

41. Joseph Menn, "Expert: Cyber-attacks on Georgia Websites Tied to Mob, Russian Government," *L.A. Times,* August 13, 2008, accessed November, 16, 2009, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

42. Kim Hart, "Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar," *Washington Post,* January 13, 2008, accessed November 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html.

43. John Markoff, "Web Becomes a Battleground in Russia-Georgia Conflict," *New York Times,* August 12, 2008, accessed November 16, 2009, http://www.nytimes.com/2008/08/12/world/europe/12iht-cyber.4.15218251.html.

44. Ibid.

45. Shaun Waterman, "Analysis: Russia-Georgia Cyberwar Doubted," *United Press International,* August 18, 2008, accessed February 27, 2010, http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyberwar_doubted_999.html.

46. Thais Portilho-Shrimpton, "Battle for South Ossetia Fought in Cyberspace," *The Independent,* August 17, 2008, accessed November 16, 2009, http://www.independent.co.uk/news/world/europe/battle-for-south-ossetia-fought-in-cyberspace-899772.html.

47. Noah Shachtman, "Estonia, Google Help 'Cyberlocked' Georgia (Updated)," *Wired Blog Network/Danger Room,* August 11, 2008, accessed November 16, 2009, http://www.wired.com/dangerroom/2008/08/civilge-the-geo.

48. Jeremy Kirk, "Update: Estonia, Poland Help Gerogia Fight Cyberattacks," *IDG News Service,* August 12, 2008, accessed November 16, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112399&source=rss_news50.

49. Alexander Melikishvili, "The Cyber Dimension of Russia's Attack on Georgia," *Eurasia Daily Monitor,* September 12, 2008, accessed November 16, 2009, http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33936.

50. Evgeny Morozov, "An Army of Ones and Zeroes," *Slate,* August 14, 2008, accessed November 16, 2009, http://www.slate.com/id/2197514/.

51. "Russia/Georgia Cyber War – Findings and Analysis, Project Grey Goose," Palantir Technologies, accessed November 16, 2009, http://palantirtech.com/greygoose/.

52. Ibid., 4.

53. Ibid.

54. CIA World Factbook, "Georgia," Central Intelligence Agency, accessed November 17, 2009, https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html/.

55. U.S. Congressional Research Service, *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* 1, by Clay Wilson, Washington, D.C., 2008, accessed November 16, 2009, http://fas.org/sgp/crs/terror/RL32114.pdf.

56. Brian M. Mazanec, "The Art of (Cyber) War," *The Journal of International Security Affairs* 16 (Spring 2009), accessed May 7, 2011, http://www.securityaffairs.org/issues/2009/16/mazanec.php.

57. Steven Metz and Douglas V. Johnson II, "Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts," USAF Center for Strategy and Technology, January 2001, 5, accessed May 7, 2011, http://www.au.af.mil/au/awc/awcgate/ssi/asymetry.pdf .

58. Bradley Graham, "Hackers Attack Via Chinese Web Sites," *Washington Post,* August 25, 2005, accessed May 7, 2011http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

59. U.S.-China Economic and Security Review Commission, *USSC 2008 Annual Report,* 162-163, accessed November 16, 2009, http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.

60. Department of Defense, *Annual Report to Congress: Military Power of the People's Republic of China 2008,* 2008, 4, accessed May 7, 2011, http://www.mcsstw.org/www/download/China_Military_Power_Report_2008.pdf.

61. Ibid.

62. Ibid.

63. *Financial Times,* "BushHackers," November 8, 2008, accessed November 16, 2009, http://www.ft.com/cms/s/0/497feb92-ad09-11dd-971e-000077b07658.html/.

64. Demetri Sevastopulo, "Chinese Hack into White House Network," *Financial Times,* November 6, 2008, accessed November 16, 2009, http://www.ft.com/cms/s/2931c542-ac35-11dd-bf71-000077b07658.html.

65. Ibid.

66. Federal Bureau of Investigation, "Cyber Crime: National Cyber Investigative Joint Task Force," accessed November 16, 2009, http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

67. U.S.-China Economic and Security Review Commission, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* by Bryan Krekel (Washington, D.C.: U.S. Government Printing Office, 2009), accessed November 16, 2009, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

68. U.S.-China Economic and Security Review Commission, *USSC 2008 Annual Report* (Washington, D.C.: U.S. Government Printing Office, 2008), 164, accessed November 16, 2009, http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.

69. Simon Elegant, "Enemies at the Firewall," *Time,* December 6, 2007, accessed November 16, 2009, http://www.time.com/time/magazine/article/0,9171,1692063,00.html/.

70. Ibid.

71. U.S.-China Economic and Security Review Commission, *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* 36.

72. Ibid.

73. U.S.-China Economic and Security Review Commission, *USSC 2008 Annual Report,* 165.

74. 60 Minutes, "Cyber War: Sabotaging the System."

75. U.S.-China Economic and Security Review Commission, *USSC 2008 Annual Report,* 167.

76. Charles W. Freeman, Jr., *Diplomatic Strategy and Tactics* (Washington D.C.: U.S. Institute of Peace, 1997): 84.

77. U.S.-China Economic and Security Review Commission, *USSC 2008 Annual Report,* 75.

78. Scott W. Beidleman, "Defining and Deterring Cyber War," United States Air Force, 2009, 20, accessed November 16, 2009, http://www.hsdl.org/?view&did=28659.

79. Sanger, Markoff, and Shanker, "U.S. Steps Up Effort on Digital Defenses."

80. Ibid.

81. Ibid.

82. Ibid.

83. John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk," *New York Times,* August 2, 2009, accessed November 16, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html/.

84. Ibid.

85. Sanger, Markoff, and Shanker, "U.S. Steps Up Effort on Digital Defenses."

86. John Markoff and Thom Shanker, "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk."

87. Ellen Nakashima, "Cybersecurity Official Resigns Over Delays in Appointment," *Washington Post,* August 4, 2009, accessed November 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/08/03/AR2009080302697.html.

88. Ibid.

89. Strategic Technology Office, "The National Cyber Range: A National Testbed for Critical Security Research," 1, accessed May 7, 2011, http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf .

90. Barack Obama, "National Strategy for Trusted Identities in Cyberspace," April 2009, accessed May 7, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

BIBLIOGRAPHY

Adams, James. "Virtual Defense." *Foreign Affairs* 80,3 (May-June 2001): 98-112.

Barber, Tony. "NATO Expels Russian Envoys." *Financial Times,* April 29, 2009. Accessed November 16, 2009, http://www.ft.com/cms/s/0/39446224-3500-11de-940a-00144feabdc0.html.

Barnes, Julian. "Cyber Attack Has Pentagon Worried." *Chicago Tribune,* November 30, 2008. Accessed November 16, 2009, http://www.chicagotribune.com/news/nationworld/chi-cyberattack_bdnov30,0,633998.story.

Beidleman, Scott W. "Defining and Deterring Cyber War." United States Air Force, 2009. Accessed November 16, 2009, http://www.hsdl.org/?view&did=28659.

Boyes, Roger. "Russian Spy in NATO Could Have Passed on Missile Defense and Cyber-War Secrets." *Times Online,* November 16, 2009. Accessed November 16, 2009http://www.timesonline.co.uk/tol/news/world/europe/article5166227.ece.

"BushHackers." *Financial Times,* November 8, 2008. Accessed November 16, 2009, http://www.ft.com/cms/s/0/497feb92-ad09-11dd-971e-000077b07658.html.

Center for Strategic International Studies. "Significant Cyber Incidents Since 2006." Working paper. November 6, 2009. Accessed November 16, 2009http://www.csis.org/files/publication/100120_CyberEventsSince2006.pdf.

CIA World Factbook. "Georgia." Central Intelligence Agency. Accessed November 17, 2009, https://www.cia.gov/library/publications/the-world-factbook/geos/gg.html.

Department of Defense. *National Defense Strategy.* June 2008. Accessed May 7, 2011, http://www.defenselink.mil/pubs/2008NationalDefenseStrategy.pdf.

Department of Defense. *Annual Report to Congress: Military Power of the People's Republic of China 2008.* Accessed May 7, 2011, http://www.mcsstw.org/www/download/China_Military_Power_Report_2008.pdf.

Dunnigan, James F. *The Next War Zone: Confronting the Global Threat of Cyberterrorism.* New York City: Kensington Publishing Corporation, 2002.

Ebinger, Charles, and Kevin Massey. "Software and Hard Targets: Enhancing Smart Grid Cyber Security in the Age of Information Warfare." *Brookings Energy Security Initiative.* February 2011. Accessed May 7, 2011, http://www.brookings.edu/~/media/Files/rc/papers/2011/02_smart_grid_ebinger/02_smart_grid_ebinger.pdf.

Elegant, Simon. "Enemies at the Firewall." *Time,* December 6, 2007. Accessed November 16, 2009, http://www.time.com/time/magazine/article/0,9171,1692063,00.html.

Farivar, Cyrus. "Cyberwar I: What the Attacks on Estonia Have Taught Us about Online Combat." *Slate,* May 22, 2007. Accessed November 16, 2009, http://www.slate.com/id/2166749/.

Federal Bureau of Investigation. "Cyber Crime: National Cyber Investigative Joint Task Force." Accessed November 16, 2009, http://www.fbi.gov/about-us/investigate/cyber/ncijtf.

Freeman, Charles W. *Diplomatic Strategy and Tactics.* Washington, D.C.: U.S. Institute of Peace, 1997.

Frontline. "Cyber War!" PBS, April 24, 2003. Accessed November 16, 2009, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/script.html.

Graham, Bradley. "Hackers Attack Via Chinese Web Sites." *Washington Post,* August 25, 2005. Accessed May 7, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2005/08/24/AR2005082402318.html.

Grant, Rebecca. "Cyber Menace." *Airforce Magazine,* March 2009, 24-27. Accessed November 16, 2009, http://www.airforce-magazine.com/MagazineArchive/Pages/2009/March%202009/0309cyber.aspx.

Hart, Kim. "Longtime Battle Lines Are Recast in Russia and Georgia's Cyberwar." *Washington Post,* January 13, 2008. Accessed November 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2008/08/13/AR2008081303623.html.

iDefense. "Cyber Espionage: China and the Network Crack Program Hacker Group." Accessed November 16, 2009, http://labs.idefense.com/intelligence/researchpapers.php.

Kirk, Jeremy. "Update: Estonia, Poland Help Georgia Fight Cyberattacks." *IDG News Service,* August 12, 2008. Accessed November 16, 2009, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9112399&source=rss_news50.

Lewis, James A. "Cyber Security – Assessing Our Vulnerabilities and Developing an Effective Defense." Statement, CSIS, Senate Committee on Commerce, Science, and Transportation, March 19, 2009. Accessed November 16, 2009, http://csis.org/files/media/csis/congress/ts090319_lewis.pdf.

Markoff, John. "Web Becomes a Battleground in Russia-Georgia Conflict." *New York Times,* August 12, 2008. Accessed November 16, 2009, http://www.nytimes.com/2008/08/12/world/europe/12iht-cyber.4.15218251.html.

Markoff, John, and Thom Shanker. "Halted '03 Iraq Plan Illustrates U.S. Fear of Cyberwar Risk." *New York Times,* August 2, 2009. Accessed November 16, 2009, http://www.nytimes.com/2009/08/02/us/politics/02cyber.html.

Mazanec, Brian M. "The Art of (Cyber) War." *The Journal of International Security Affairs* 16 (Spring 2009). Accessed May 7, 2011, http://www.securityaffairs.org/issues/2009/16/mazanec.php.

Melikishvili, Alexander. "The Cyber Dimension of Russia's Attack on Georgia." *Eurasia Daily Monitor,* September 12, 2008. Accessed November 16, 2009, http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33936.

Menn, Joseph. "Expert: Cyber-attacks on Georgia Websites Tied to Mob, Russian Government." *L.A. Times,* August 13, 2008. Accessed November, 16, 2009, http://latimesblogs.latimes.com/technology/2008/08/experts-debate.html.

Metz, Steve,n and Douglas V. Johnson II. "Asymmetry and U.S. Military Strategy: Definition, Background, and Strategic Concepts." USAF Center for Strategy and Technology, January 2001. Accessed May 7, 2011, http://www.au.af.mil/au/awc/awcgate/ssi/asymetry.pdf.

Morozov, Evgeny. "An Army of Ones and Zeroes." *Slate,* August 14, 2008. Accessed November 16, 2009, http://www.slate.com/id/2197514/.

Nakashima, Ellen. "Cybersecurity Official Resigns Over Delays in Appointment." *Washington Post,* August 4, 2009. Accessed November 16, 2009, http://www.washingtonpost.com/wp-dyn/content/article/2009/08/03/AR2009080302697.html.

National Intelligence Council. *Global Trends 2025: A Transformed World.* Washington, D.C.: U.S. Government Printing Office, 2008. Accessed November 16, 2009, http://www.dni.gov/nic/NIC_2025_project.html.

Obama, Barack. "National Strategy for Trusted Identities in Cyberspace." April 2009. Accessed May 7, 2011, http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf.

Organisation for Economic Co-operation and Development. "Malicious Software (Malware): A Security Threat to the Internet Economy." Ministerial Background Report DSTI/ICCP/REG(2007)5/FINAL, June 2008. Accessed May 7, 2011, http://www.oecd.org/dataoecd/53/34/40724457.pdf.

Owens, William A., Kenneth W. Dam, and Herbert S. Lin. *Technology, Policy, Law, and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities.* Washington, D.C.: National Academies Press, 2009.

Portilho-Shrimpton, Thais. "Battle for South Ossetia Fought in Cyberspace." *The Independent,* August 17, 2008. Accessed November 16, 2009, http://www.independent.co.uk/news/world/europe/battle-for-south-ossetia-fought-in-cyberspace-899772.html.

"Russia/Georgia Cyber War – Findings and Analysis, Project Grey Goose." Palantir Technologies. Accessed November 16, 2009, http://palantirtech.com/greygoose.

Ryan, Johnny. "iWar: A New Threat, Its Convenience, and Our Increasing Vulnerability." *NATO Review,* Winter 2007. Accessed November 16, 2009, http://www.nato.int/docu/review/2007/issue4/english/analysis2.html.

Sanger, David E., John Markoff, and Thom Shanker. "U.S. Steps Up Effort on Digital Defenses." *New York Times,* April 28, 2009. Accessed November 16, 2009, http://www.nytimes.com/2009/04/28/us/28cyber.html.

Schwirtz, Michael. "Former Estonian Official Convicted of Treason." *New York Times,* February 25, 2009. Accessed November 16, 2009, http://www.nytimes.com/2009/02/26/world/europe/26estonia.html.

Sevastopulo, Demetri. "Chinese Hack into White House Network." *Financial Times,* November 6, 2008. Accessed November 16, 2009, http://www.ft.com/cms/s/2931c542-ac35-11dd-bf71-000077b07658.html.

Shachtman, Noah. "Estonia, Google Help 'Cyberlocked' Georgia (Updated)." *Wired Blog Network/Danger Room,* August 11, 2008. Accessed November 16, 2009, http://www.wired.com/dangerroom/2008/08/civilge-the-geo/.

Socor, Vladimir. "NATO Creates Cyber Defense Center in Estonia." *Eurasia Daily Monitor,* May 15, 2008. Accessed November 16, 2009, http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=33636.

Strategic Technology Office. "The National Cyber Range: A National Testbed for Critical Security Research." Accessed May 7, 2011, http://www.whitehouse.gov/files/documents/cyber/DARPA%20-%20NationalCyberRange_FactSheet.pdf.

Traynor, Ian. "Russia Accused of Unleashing Cyberwar to Disable Estonia." *The Guardian,* May 17, 2007. Accessed November 16, 2009, http://www.guardian.co.uk/world/2007/may/17/topstories3.russia.

U.S.-China Economic and Security Review Commission. *Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation,* by Bryan Krekel. Washington, D.C.: U.S. Government Printing Office, 2009. Accessed November 16, 2009, http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf.

U.S.-China Economic and Security Review Commission. *USSC 2008 Annual Report*. Washington, D.C.: U.S. Government Printing Office, 2008. Accessed November 16, 2009, http://www.uscc.gov/annual_report/2008/annual_report_full_08.pdf.

U.S. Congressional Research Service. *Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress,* by Clay Wilson. Washington, D.C., 2008. Accessed November 16, 2009, http://fas.org/sgp/crs/terror/RL32114.pdf.

U.S. General Accountability Office. "Hybrid Warfare." GAO-10-1036R, September 10, 2010. Accessed May 7, 2011, http://www.gao.gov/products/GAO-10-1036R.

Waterman, Shaun. "Analysis: Russia-Georgia Cyberwar Doubted." *United Press International,* August 18, 2008. Accessed February 27, 2010, http://www.spacewar.com/reports/Analysis_Russia-Georgia_cyberwar_doubted_999.html.

Enriching Lives, Preserving the Planet: *Sustainable Development in South Africa*

Todd Smith

For at least the past 20 years humankind has been living in a manner that our planet is incapable of sustaining indefinitely. We have been consuming resources faster than the earth can replenish them and we have been emitting wastes faster than the earth can absorb them. Essentially, we have been living beyond our ecological means and, while the Earth will continue unabated, we will eventually render it uninhabitable by humankind.

According to the now widely accepted methodology of ecological footprinting developed by Wackernagel and Rees,[1] and calculated today by the Global Footprint Network (GFN) led by Wackernagel, the world used 2.7 global hectares per person (gha/p) in 2005—our ecological footprint—while the earth's available resources—its global biocapacity—amounted to only 2.1 GHP. In other words, it would take 1.3 Earths to continue to support the world's population at its current rate of resource consumption. This situation is known as *ecological overshoot*.[2]

Sustainable Development: A Theoretical Framework

Most organizations, public or private, that focus on economic development or poverty reduction are concerned primarily with creating jobs and raising the income of the poor in the belief that this in the best way to improve the living conditions of the poor. They should, however, focus more attention on environmental issues for two reasons. First, improving the environmental health conditions within impoverished communities can, on its own, improve the living conditions of the poor. Second, impoverished countries and communities, while not without some responsibility for environmental degradation, always suffer the consequences of unsustainable resource use earlier and more severely than those better positioned to adapt to changing conditions created by disappearing resources. In other words,

the brunt of environmental hazards borne by the poor is disproportionate to their contribution to environmental degradation.

The GFN elucidates the situation succinctly. "Human demand on ecosystems can exceed biocapacity for some time, by liquidating resource stocks, and allowing wastes, such as carbon dioxide, to accumulate in the biosphere. As overshoot continues, fisheries will collapse, surface water and groundwater will become scarce, and forest will disappear. A reduction in available resources will translate into enormous human suffering, which will first affect those who cannot immigrate to more plentiful regions, or afford to import increasingly expensive necessities."[3]

The specific challenges faced by the poor are numerous and interrelated.

- The poor frequently pay disproportionate sums for inadequate water supply. This combined with poor sanitation services in disadvantaged areas leads to the spread of diarrheal diseases and, consequently, increased health care expenditures and decreased economic production. Furthermore, children, especially girls, are often kept out of school because of the need to collect water and carry it long distances. They are, therefore, relegated to a future of illiteracy and poverty.[4]

- Rising food prices have an obvious and disproportionate impact on impoverished families who devote a larger share of their income to nutrition.[5] Among the many contributing factors to rising food prices are drought and decreased rainfall that may be an initial symptom of climate change, increased transportation costs due to rising oil prices, and competition for crops to support the growing biofuel market.[6]

- Poor air quality in areas surrounding industrial polluters and often inhabited by the urban poor leads to respiratory diseases, which lead to increased health costs and loss of economic potential.

- Loss of biodiversity (caused by over-taking, habitat destruction, or introduction of alien species), soil erosion and nutrient depletion, and deforestation are all increasing at an alarming rate. Among the tragic consequences of these factors are the failure of ecosystems and the loss of productive farmland upon which rural populations rely.

- Impending climate change widely attributed to unsustainable emissions of carbon dioxide and other greenhouse gases will have a wide variety of detrimental effects on the world's poor. In its most recent Human Development Report the United Nations Development Programme (UNDP) identified "five specific risk-multipliers for human development reversals," many of which have already been mentioned. These "risk-multipliers" are reduced agricultural productivity, heightened water insecurity, increased exposure to coastal flooding and extreme weather events, the collapse of ecosystems, and increased health risks.[7]

This list is hardly exhaustive. It is, however, illustrative of the interconnectedness of the mechanisms through which disadvantaged communities are further impoverished by unsustainable resource use.

Effective poverty alleviation, therefore, relies in part on protection and conservation of the Earth's ecological resources and on economic development programs that do not squander those resources. Known today as *sustainable development,* this concept was first embraced in 1987 by the United Nations World Commission on Environment and Development when it wrote in its final report, *Our Common Future:* "Sustainable development is development that meets the needs of the present generation without compromising the ability of future generations to meet their own needs."[8]

The concept has been increasingly accepted in the past 20 years and has been the subject of several international conferences. The 1992 United Nations Conference on Environment and Development held in Rio de Janeiro resulted in the adoption of *Agenda 21,* still considered, 16 years later, to be the quintessential framework for sustainable development. The first paragraph of the Preamble to *Agenda 21* reads:

> Humanity stands at a defining moment in history. We are confronted with a perpetuation of disparities between and within nations, a worsening of poverty, hunger, ill health and illiteracy, and the continuing deterioration of the ecosystems on which we depend for our well-being. However, integration of environment and development concerns and greater attention to them will lead to the fulfillment of basic needs, improved living standards for all, better protected and managed ecosystems and a safer, more prosperous future. No nation can achieve this on its own; but together we can—in a global partnership for sustainable development.[9]

Still, sustainable development is hardly universally accepted. The perspective of "sustainable resource use as precondition for poverty eradication" is in stark contrast to the persistently predominant perspective amongst many developmental economists who promote poverty reduction through economic development first, followed by environmental clean-up later.[10] The danger inherent in the latter approach is that short-term economic gains will, in the long-term, be outweighed by the lasting consequences of unsustainable resource use. "Effective management of ecological assets can help end cycles of poverty and can support changes, like those called for in the Millennium Development Goals, that improve quality of life. In contrast, gains built on liquidating ecosystems will only be short lived, and poorer countries will be most at risk of suffering the consequences."[11]

GLOBAL CONTEXT: DIFFERENT OBSTACLES FOR DIFFERENT COUNTRIES

Obviously, all countries are not alike. Wealthy countries use far more than their fair share of the world's limited environmental resources, while poorer countries are forced to suffer more than their fair share of the consequences of global overshoot. The Global Footprint Network has pioneered a revealing tool to assess a

country's progress toward sustainability. This measure plots a country's previously discussed ecological footprint against its human development index (HDI), a measure of well-being created by the UNDP using life expectancy, literacy and education, and per capita gross domestic product and normalized to a score between zero and one. Only a few countries meet the minimum criteria for sustainability: high human development, an HDI of over .8; and a sustainable ecological footprint, less than 2.1 GHP.

The rich developed nations of North America and the European Union have a high HDI accompanied by a large ecological footprint. The United States consumes an alarming 9.6 GHP. These countries are faced with the challenge of reducing their consumption of resources while maintaining their high level of development. A reduction in resource consumption will undoubtedly rely on a combination of strategies. Technological innovation, most notably in the area of sustainable or renewable energy sources, is vitally important and research into new technologies should be vigorously pursued. Technological advances, however, will not be enough. Improved conservation of dwindling resources must be a priority and will require a mix of governmental regulation and market mechanisms to change individual behavior.

At the other extreme, most countries in sub-Saharan Africa have sustainable ecological footprints but the lowest human development in the world. The average footprint of all sub-Saharan Africa is less than one GHP. This is not to imply that these countries are somehow more ecologically responsible than the rest of the world. Rather, in very simplistic terms, ecological footprint is a function of consumption levels and poor countries consume less. These countries face a very different challenge. They must increase human development while maintaining sustainable levels of resource use. This is an unprecedented challenge that requires original thinking and innovative models of development. As noted above, the old model of industrialization followed by environmental clean-up is no longer an option that can be expected to yield long-term dividends.

Beyond the obvious injustice of this state of affairs, it creates seemingly intractable obstacles to global cooperation. But cooperate we must. In 2002, the international community met in Johannesburg for the World Summit on Sustainable Development (WSSD). South Africa, as the host country, focused much of the attention of the conference on poverty reduction. The main document to result from this conference was the Johannesburg Plan of Implementation which states:

> *Eradicating poverty is the greatest global challenge facing the world today and an indispensable requirement for sustainable development, particularly for developing countries.* Although each country has the primary responsibility for its own sustainable development and poverty eradication and the role of national policies and development strategies cannot be overemphasized, concerted and concrete measures are required at all levels to enable developing countries to achieve their sustainable development goals as related to the internationally agreed poverty-related targets and goals, including those contained in Agenda 21, the relevant

outcomes of other United Nations conferences and the United Nations Millennium Declaration.[12]

While it is true that poverty, especially urban poverty, and environmental degradation are intricately linked, it is not true that ecological sustainability cannot be obtained until poverty is eradicated. Advocates of this proposition consider poverty to be the cause of ecological collapse. As will be demonstrated, the converse is more accurate. Environmental hazards are a major contributing factor to poverty. Consequently, sustainable use of ecological resources is a prerequisite of poverty reduction. Attaining international goals for poverty reduction will require considerable progress toward sustainability through industrious and innovative programs on the national and local levels in conjunction with global cooperation. In the words of a 13-year-old girl from the Cape Flats, "We need everyone to work together to take care of the environment."[13]

SOUTH AFRICAN CONTEXT: A UNIQUE PREDICAMENT

Nowhere is the complex relationship between poverty and the environment more evident than in the context of South Africa. South Africa has an HDI of 0.67,[14] below the established minimum for high development, and an unsustainable ecological footprint of 2.3 GHP.[15] This somewhat unique situation is a function of the vast inequality in this country—South Africa has one of the world's most unequal wealth distributions.[16] Unsurprisingly, its consumption of ecological resources is likewise strikingly unequal. A sizable minority in South Africa matches the high human development of the world's richest nations as well as the accompanying unsustainable ecological footprint. A much larger segment of the population, however, rivals the stunted human development of its sub-Saharan neighbors and the small footprint corresponding to their lower consumption levels.[17]

A recent study by Mark Swilling examined the different footprints of the widely divergent neighborhoods of Cape Town. He found that the wealthiest households—the top 7 percent—had an ecological footprint of 14.8 GHP and the upper-middle class neighborhoods—the next 9 percent—consumed 5.8 GHP. In contrast, the bottom 51 percent of households—those living in the townships or informal settlements—had an ecological footprint of a mere one GHP or less.[18]

ENVIRONMENTAL HAZARDS AND ENVIRONMENTAL DEGRADATION

Again, this is not to suggest that the poor live environmentally idyllic lifestyles. One has only to visit one of the many informal settlements in South Africa's urban centers to observe the numerous environmental hazards that confront the residents every day. Inadequate sanitation and polluted water sources, overcrowded housing, accumulated solid waste, poor air quality, deforested landscape, and degraded soil are often characteristics of these areas. Furthermore, these informal settlements are often located in areas that are more susceptible to natural disasters, particularly flooding, the effects of which are often intensified by these environmental hazards. It is often assumed that this environmental degradation is linked to or even a product of urban poverty. More accurately, however, these

environmental hazards are a contributing factor to urban poverty. The key distinction here is the difference between environmental degradation and environmental hazards.

> At the core of most misunderstandings about the link between poverty and environment is the confusion between environmental hazards and environmental degradation. In most urban centers in Africa, Asia, and Latin America, a high proportion of the poor (however defined) face very serious environmental hazards in their homes and their surrounds and in their workplaces. Such hazards impose large burdens on such groups in terms of ill health, injury, and premature death. These health burdens are a major cause or contributor to poverty. But most of these environmental hazards are not causing environmental degradation. For instance, the inadequacies in provision for piped water, sanitation, and drainage in most low- income neighborhoods often mean very serious problems with insect-borne diseases such as malaria or dengue fever or filariasis and with diseases associated with a lack of water for washing such as trachoma, but these do not degrade any environmental resource.[19]

Environmental degradation is more accurately understood in this context as a function of urban growth rates that are outpacing the extension of infrastructure and services to the urban poor. In other words, it is not the inhabitants of informal settlements that are culpable for environmental degradation. All people, regardless of income, have the same basic needs. Inadequate water provision causes unsustainable use of limited or polluted sources because people need water; lack of sanitation facilities causes pollution of those same water sources because people need to defecate; lack of rubbish collection services causes solid waste accumulation because people create waste; failure to properly plan for growth causes untenable land-use, deforestation and species loss because people need space and building materials; inadequate provision of electricity also causes deforestation and species loss, as well as unsustainable carbon emissions because people need wood for heating and cooking fuel.[20] The causes of environmental degradation, therefore, are more properly viewed as failures of governance.[21]

REDEFINING POVERTY . . . AND POVERTY REDUCTION

Next, it is important to understand that inadequate income or consumption is not a satisfactory definition of poverty. Satterthwaite presents a broader conception of poverty that incorporates eight interrelated sets of deprivations:

1. Inadequate income (and thus inadequate consumption of necessities including food) and often problems of indebtedness, with debt repayments significantly reducing the income available for necessities.
2. Inadequate, unstable, or risky asset base (nonmaterial and material including educational attainment and housing) for individuals, households, or communities. Different assets have different roles. For instance, some are important for generating or maintaining income, some are important

for helping low-income people cope with economic stresses or shocks, and some are important for limiting environmental hazards that can have serious health and economic costs.

3. Inadequate shelter that is typically of poor quality, overcrowded and often insecure (because of no protection from eviction by landlords or landowners).

4. Inadequate provision of public infrastructure (piped water, sanitation, drainage, roads, footpaths, etc.).

5. Inadequate provision of basic services such as day care and schools, health care, emergency services, public transport, communications, and law enforcement.

6. Limited or no safety net to ensure that basic consumption can be maintained when income falls and to ensure access to shelter and health care when these can no longer be paid for.

7. Inadequate protection of poorer groups' rights through the operation of the law, including laws and regulations regarding civil and political rights, occupational health and safety, pollution control, environmental health, protection from violence and other crimes, and protection from discrimination and exploitation.

8. Poorer groups' silence and powerlessness within political systems and bureaucratic structures, leading to little or no possibility of receiving entitlements; of organizing, making demands, and getting a fair response; and of receiving support for developing their own initiatives. Also, no means of ensuring accountability from aid agencies, nongovernmental organizations (NGOs), public agencies, and private utilities and an inability to participate in the definition and implementation of their urban poverty programs.[22]

Using these criteria, it is easy to see that poverty is most concentrated in, but not exclusive to, urban informal settlements. Mark Napier, who has extensively studied poverty, informal settlements, and the environment in South Africa, writes, "Certainly given definitions of poverty that are not simply generated by counting household incomes, by definition the lack of access to adequate shelter, water, sanitation, drainage and solid waste removal which accompanies the occupation of unconsolidated and un- or under-serviced informal settlements means that human poverty is indeed concentrated very explicitly in such settlements."[23]

It is shortsighted and narrow-minded to think of poverty reduction—or improved human development—merely in terms of creating new jobs. Ironically, it is the draw of better economic opportunities—jobs—that often brings the poor to urban centers and thereby exacerbates the environmental hazards prevalent in informal settlements where these newcomers settle. The creation of new jobs in an area may provide additional income to a community and accordingly raise con-

sumption, but without access to basic services the real conditions of poverty will remain unchanged and, indeed, may worsen.

Conversely, it is possible to alleviate the conditions of poverty without increasing income.[24] By discovering or developing creative and innovative methods to improve service delivery, it is possible to overcome the environmental hazards that deepen the poverty of millions of South Africans. By taking action in the absence of public service delivery, NGOs, governmental departments, and ordinary people are improving their own situation and that of their fellow citizens. It is in this context that many of the innovative programs presented in this booklet are effectively improving the lives of those living in impoverished areas and, thereby, alleviating poverty.[25]

Of course, it is still essential that the disproportionate consumption of ecological resources of the rich and middle-class be reduced drastically if sustainability is to be achieved. "Indeed, the key relationship between environmental degradation and urban development is in regard to the consumption patterns of non-poor urban groups (especially high-income groups) and the urban-based production and distribution systems that serve them."[26]

Failure to properly address this inequality in resource use can also be viewed as a failure in governance resulting from shortsightedness and a breakdown in the linkage between overall government expenditure and environmental wellbeing. For example, disease and other health problems caused by poor sanitation and poor air quality lead directly to increased and inefficient healthcare expenditures. The restoration of this connection should be a primary focus of local poverty reduction initiatives. By emphasizing these linkages, organizations or municipalities can foster direct cooperation between all interested stakeholders and improve the ecological sustainability of the entire community.

Additionally, local municipal and civil society programs can contribute indirectly to more equitable and sustainable resource use. As impoverished communities take action to protect the local environment, they gain an increased understanding of the importance of conservation and sustainable resource use and consequences of unsustainable resource, the preponderance of which they suffer. This new understanding emboldens these communities to demand governmental action or increased responsibility from other sectors of the community. People who invest time and energy into creating new green spaces are more likely to be incensed at polluting industries. People who take responsibility for managing their own water use are more likely to demand change from other irresponsible users. The problem remains, however, of ensuring political access to groups that for social or economic reasons may be totally or partially disenfranchised.

CONCLUSION

Ultimately, what is needed is a much more holistic approach if the lives of the millions of South Africans living in extreme poverty are to be improved. Unsustainable resource use must be addressed and curtailed in an economically feasible manner. Economic development programs must be designed and implemented in

an ecologically sustainable manner. As mentioned above, any policy that aims to increase human development at the expense of the environment will exacerbate the predicament of the poor and, by extension, all of South Africa. In short, ecological sustainability must be required of any undertaking, public or private. Although rarely attained, this holistic approach is encapsulated in South Africa's statutory definition of sustainable development: "Sustainable development means the integration of social, economic and environmental factors into planning, implementation and decision-making so as to ensure that development serves present and future generations."[27] Until local governments and civil society organizations internalize this definition, effective poverty alleviation will remain an elusive and unattainable goal.

ENDNOTES

1. Mathis Wackernagel and William E. Rees, *Our Ecological Footprint: Reducing Human Impact on the Earth* (Philadelphia: New Society Publishers, 1996).

2. "The Ecological Footprint is a measure of the demand human activity puts on the biosphere. More precisely, it measures the amount of biologically productive land and water area required to produce all the resources an individual, population, or activity consumes, and to absorb the waste they generate, given prevailing technology and resource management practices. This area can then be compared with biocapacity, the amount of productive area that is available to generate these resources and to absorb the waste." Brad Ewing, et al., *The Ecological Footprint Atlas 2008,* Research and Standards Department, Global Footprint Network (Oakland, CA: Global Footprint Network, 2008): 3-4.

   "Humanity as a whole, however, is not living within the means of the planet. In 2005, humanity's total Ecological Footprint worldwide was 17.5 billion global hectares (gha); with world population at 6.5 billion people, the average person's Footprint was 2.7 global hectares. But there were only 13.6 billion gha of biocapacity available that year, or 2.1 gha per person. This overshoot of almost 30 percent means that in 2005 humanity used the equivalent of 1.3 Earths to support its consumption (Figure 3). It took the Earth approximately a year and four months to regenerate the resources used by humanity in that year." Ibid., 13.

3. Global Footprint Network, "Africa's Ecological Footprint: Human Well-Being and Biological Capital," *Global Footprint Network,* November 10, 2006, accessed June 20, 2008, http://www.footprintnetwork.org/africa.

4. The United Nations Development Programme (UNDP) focused on this problem in its 2006 Human Development Report. United Nations Development Programme, *Human Development Report 2006 - Beyond scarcity: Power, poverty and the global water crisis* (New York: Palgrave Macmillan, 2006).

5. "'The surge in food prices could push 100 million people into deeper poverty,' World Bank President Robert B. Zoellick said at the International Monetary Fund-World Bank Spring Meetings in Washington. 'Based on a very rough analysis, we estimate that a doubling of food prices over the last three years could potentially push 100 million people in low income countries deeper into poverty,' Zoellick said. 'This is not just a question of short-term needs, as important as those are; this is ensuring that future generations don't pay a price too.'" The World Bank, "Food Price Crisis Imperils 100 Million in Poor Countries, Zoellick Says," *The World Bank: News & Broadcast,* April 14, 2008, accessed June 24, 2008, http://web.worldbank.org/WBSITE/EXTERNAL/NE

WS/0,,contentMDK:21729143~menuPK:34457~pagePK:34370~piPK:34424~theSitePK:4607,00.html .

6. There is significant debate regarding the effects of biofuels on food prices versus their necessity to reduce carbon emissions and dependence on fossil fuels. For a thorough discussion of this issue in the context of the US market refer to the following sources: C. Ford Runge and Benjamin Senauer, "How biofuels could starve the poor," *Foreign Affairs* 86, no. 3 (May/June 2007): 41-53; Tom Daschle, C. Ford Runge, and Benjamin Senauer, "Food for Fuel?," *Foreign Affairs* 86, no. 5 (September/October 2007): 152-162; and C. Ford Runge and Benjamin Senauer, "How Ethanol Fuels the Food Crisis," *ForeignAffairs.org,* May 28, 2008, accessed June 24, 2008, http://www.foreignaffairs.org/20080528faupdate87376/c-ford-runge-benjamin-senauer/how-ethanol-fuels-the-food-crisis.html.

7. United Nations Development Programme, *Human Development Report 2007/2008 - Fighting climate change: Human solidarity in a divided world* (New York: Palgrave Macmillan, 2007).

8. World Commission on Environment and Development, *Our Common Future* (Oxford and New York, Oxford University Press, 1987).

9. United Nations, "Agenda 21," *United Nations Sustainable Development,* 1992, accessed June 20, 2008, http://www.un.org/esa/sustdev/documents/agenda21/english/Agenda21.pdf.

10. Mark Swilling, "Local Governance and the Politics of Sustainability," in *Consolidating Developmental Local Government: Lessons for the South African Experience* (Cape Town: UCT Press, 2008): 77-107

11. Steven Goldfinger, et al., "Africa: Ecological Footprint and Human Well-being," ed. Steven Goldfinger (Gland, Switzerland: WWF-World Wildlife Fund For Nature, June 2008): 3.

12. World Summit on Sustainable Development, UN Department of Economic and Social Affairs: Division for Sustainable Development, *Documents: Johannesburg Plan of Implementation,* August 11, 2005, accessed June 24, 2008, http://www.un.org/esa/sustdev/documents/WSSD_POI_PD/English/POIToc.htm.

13. Kimico, Nadine, Riana and Zaeedah, interview by Todd G. Smith, West End Primary School, Mitchells Plain, June 27, 2008.

14. United Nations Development Programme, *Human Development Reports,* 2008, accessed June 23, 2008, http://hdrstats.undp.org/countries/data_sheets/cty_ds_ZAF.html.

15. Global Footprint Network, "Africa: Ecological Footprint and Human Well-being," Global Footprint Network, 2008, accessed June 20, 2008, http://www.footprintnetwork.org/africa.

16. At 57.8, South Africa's GINI coefficient, a measurement of income inequality, is the tenth highest in the world according to the UNDP. United Nations Development Programme, *2007/2008 Report: Ineqality in income or expenditure,* 2008, accessed August 12, 2008, http://hdrstats.undp.org/indicators/147.html.

17. According to the United Nations Development Programme, 34 percent of the population of South Africa, 16.3 million people, lives on less than two US dollars per day. United Nations Development Programme, *Human Development Reports,* 2008, accessed June 23, 2008, http://hdrstats.undp.org/countries/data_sheets/cty_ds_ZAF.html.

18. Mark Swilling, "Sustainability and Infrastructure Planning in South Africa: A Cape Town Case Study," *Environment and Urbanization* 18,1 (April 2006): 23-50.

19. David Satterthwaite, "The Links between Poverty and the Environment in Urban Areas of Africa, Asia, and Latin America," *Annals of the American Academy of Political and Social Science* 590,1 (November 2003): 73-92.

20. Water pollution, solid waste accumulation and soil degradation in poor communities are undoubtedly local environmental hazards but not environmental degradation on a national or global scale. In contrast, unsustainable consumption of wood for heating and cooking fuel can lead to deforestation as well as unmitigated carbon emissions. These are indeed degradations that can and do impact non-local and global ecosystems. A study published in 1994, Berry et al. found that informal settlements contributing significantly to loss of coastal vegetation in South Africa's south-eastern Cape. M.G. Berry, B.L. Robertson and E.E. Campbell, "Impacts of Informal Settlements on South-Eastern Cape Coastal Vegetation (South Africa)," *Global Ecology and Biogeography Letters* 4,5 (September 1994): 129-139.

21. "A failure of governance underlies most environmental problems-failures to control industrial pollution and occupational exposure, to promote environmental health, to ensure that city dwellers have the basic infrastructure and services essential for health and a decent living environment, to plan in advance to ensure sufficient land is available for housing developments for low-income groups, and to implement preventive measures, to avoid urban sprawl." David Satterthwaite, "The Links between Poverty," 73-92.

22. Ibid.

23. Mark Napier, "Informal settlement integration, the environment and sustainable livelihoods in sub-Saharan Africa," Programme for Sustainable Human Settlements, Council for Scientific and Industrial Research (CSIR), South Africa, 2003, accessed June 23, 2008, http://schant.socialdev.net/data/Portals/www.livelihoods.org/napier.PDF.

24. "A growing number of case studies show how the deprivations associated with low income can be much reduced without increasing incomes through improving infrastructure and services or through political changes, which allowed low-income groups to negotiate more support." David Satterthwaite, "The Links between Poverty." 73-92.

25. Satterthwaite divides innovations of this type into two categories. "The first is the innovation shown by particular city authorities in developing and implementing their own local agendas. . . . The second is the innovation shown by local NGOs working with organizations of the urban poor-sometimes working with government, sometimes working in the absence of government. . . ." Ibid.

26. Ibid.

27. National Environmental Management Act [No. 107 of 1998], South Africa, 1998.

BIBLIOGRAPHY

Berry, M.G., B.L. Robertson, and E.E. Campbell. "Impacts of Informal Settlements on South-Eastern Cape Coastal Vegetation (South Africa)." *Global Ecology and Biogeography Letters* 4,5 (September 1994):129-139.

Daschle, Tom, C. Ford Runge, and Benjamin Senauer. "Food for Fuel?" *Foreign Affairs* 86,5 (September/October 2007): 152-162.

Ewing, Brad, Steven Goldfinger, Mathis Wackernagel, Meredith Stechbart, Sarah M. Rizk, Anders Reed, and Justin Kitzes. *The Ecological Footprint Atlas 2008,* Research and Standards Department, Global Footprint Network. Oakland, CA: Global Footprint Network, 2008.

Ford Runge, C., and Benjamin Senauer. "How Ethanol Fuels the Food Crisis." ForeignAffairs.org. May 28, 2008. Accessed June 24, 2008http://www.foreignaffairs.org/20080528faupdate87376/c-ford-runge-benjamin-senauer/how-ethanol-fuels-the-food-crisis.html.

Ford Rungem, C., and Benjamin Senauer. "How biofuels could starve the poor." *Foreign Affairs* 86,3 (May/June 2007): 41-53.

Global Footprint Network, "Africa: Ecological Footprint and human well-being," Global Footprint Network. 2008. Accessed June 20, 2008, http://www.footprintnetwork.org/africa.

Global Footprint Network. "Africa's Ecological Footprint: Human Well-Being and Biological Capital." Global Footprint Network. November 10, 2006. Accessed June 20, 2008, http://www.footprintnetwork.org/africa.

Goldfinger, Steven, Mathis Wackernagel, Shiva Niazi, Audrey Peller, Martin Kaercher, Justin Kitzes, Brad Ewing, Francesca Silvestri, Kristine Hayes, Tomonori Wakabayashi. "Africa: Ecological Footprint and Human Well-being." Ed. Steven Goldfinger. Gland, Switzerland: WWF-World Wildlife Fund for Nature, June 2008.

Kimico, Nadine, Riana and Zaeedah. Interview by Todd G. Smith. West End Primary School, Mitchells Plain, June 27, 2008.

Napier, Mark. "Informal settlement integration, the environment and sustainable livelihoods in sub-Saharan Africa." Programme for Sustainable Human Settlements, Council for Scientific and Industrial Research (CSIR). South Africa. 2003. Accessed June 23, 2008, http://schant.socialdev.net/data/Portals/www.livelihoods.org/napier.PDF.

National Environmental Management Act [No. 107 of 1998]. South Africa. 1998.

Satterthwaite, David. "The Links between Poverty and the Environment in Urban Areas of Africa, Asia, and Latin America." *Annals of the American Academy of Political and Social Science* 590,1 (November 2003): 73-92.

Swilling, Mark. "Local Governance and the Politics of Sustainability." In *Consolidating Developmental Local Government: Lessons for the South African Experience.* Cape Town: UCT Press, 2008.

Swilling, Mark. "Sustainability and Infrastructure Planning in South Africa: A Cape Town Case Study." *Environment and Urbanization* 18, (April 2006): 23-50.

The World Bank. "Food Price Crisis Imperils 100 Million in Poor Countries, Zoellick Says." The World Bank: News & Broadcast. April 14, 2008. Accessed June 24, 2008http://web.worldbank.org/WBSITE/EXTERNAL/NEWS/0,,contentMDK:21729143~menuPK:34457~pagePK:34370~piPK:34424~theSitePK:4607,00.html.

United Nations Development Programme, *2007/2008 Report: Inequality in income or expenditure.* 2008. Accessed August 12, 2008, http://hdrstats.undp.org/indicators/147.html.

United Nations Development Programme. *Human Development Report 2006 - Beyond Scarcity: Power, Poverty and the Global Water Crisis.* New York: Palgrave Macmillan, 2006.

United Nations Development Programme. *Human Development Report 2007/2008 - Fighting Climate Change: Human solidarity in a divided world.* New York: Palgrave Macmillan, 2007.

United Nations Development Programme. *Human Development Reports.* 2008. Accessed June 23, 2008, http://hdrstats.undp.org/countries/data_sheets/cty_ds_ZAF.html.

United Nations. "Agenda 21." *United Nations Sustainable Development.* 1992. Accessed June 20, 2008, http://www.un.org/esa/sustdev/documents/agenda21/english/Agenda21.pdf.

Wackernagel, Mathis, and William E. Rees, *Our Ecological Footprint: Reducing human impact on the Earth.* Philadelphia: New Society Publishers, 1996.

World Commission on Environment and Development, *Our Common Future.* Oxford and New York, Oxford University Press, 1987.

World Summit on Sustainable Development, UN Department of Economic and Social Affairs, Division for Sustainable Development. *Documents: Johannesburg Plan of Implementation.* August 11, 200. Accessed June 24, 2008, http://www.un.org/esa/sustdev/documents/WSSD_POI_PD/English/POIToc.htm.