Defense & Technology Paper 107

Shifting Human Environment:

How Trends in Human Geography Will Shape Future Military Operations

Paul T. Bartone & Mitchell Armbruster
Editors

CENTER FOR TECHNOLOGY AND NATIONAL SECURITY POLICY

Shifting Human Environment:

How Trends in Human Geography Will Shape Future Military Operations

Paul T. Bartone & Mitchell Armbruster

Editors

Center for Technology and National Security Policy

Institute for National Strategic Studies

National Defense University

About the authors

Mitch Armbruster

Mitch Armbruster is a Research Assistant at the Center for Technology and National Security Policy, Institute for National Strategic Studies, National Defense University. His work supports futures research and U.S. national security policy. He is a Ph.D. candidate at the Catholic University of America, focusing on the security studies, alliance politics, and politics in the Middle East. Mitch's dissertation examines how small members of an alliance can persuade their great power allies regarding threats. He holds an M.A. in politics from Catholic University and a B.A. in political science from the University of California, Los Angeles.

Dr. Paul Bartone

Colonel (Retired) Paul T. Bartone, Ph.D. is a Senior Research Fellow at the Center for Technology and National Security Policy, Institute for National Strategic Studies, National Defense University. Dr. Bartone's research focuses on understanding and measuring resilient or "hardy" responding to stress, identifying underlying biomarkers for resilience, and applying this knowledge to improve selection, training and leader development programs. While on active duty, Bartone served as the Consultant to the Surgeon General for Research Psychology, and the Assistant Corps Chief for Medical Allied Sciences. He is past-President of the American Psychological Association's Division 19 – Society for Military Psychology, a Fellow of the American Psychological Association and the Inter-University Seminar on Armed Forces and Society, and a charter member of the Association for Psychological Science. Dr. Bartone holds an M.A. and Ph.D. in Psychology and Human Development from the University of Chicago.

Dr. James Keagle

Colonel (Retired) James M. Keagle, Ph.D. is the Director of the Emerging Challenges program at the Center for Technology and National Security Policy, Institute for National Strategic Studies, National Defense University. Prior to this position, Dr. Keagle served for nine years as the National Defense University's Provost (effective 2004) and Vice President for Academic Affairs (effective 1999). While on active duty in the Air Force, Dr. Keagle served as a munitions maintenance officer, an assistant professor of political science at the Air Force Academy, and tours in political-military assignments that included direct access and interaction with Cabinet-level government officials on national security related matters. Dr. Keagle holds a B.S. from the Air Force Academy, a M.A. from the University of Pittsburg, and a M.A. and Ph.D. from Princeton University.

Celina Realuyo

Celina Realuyo is Professor of Practice at the William J. Perry Center for Hemispheric Defense Studies at the National Defense University (NDU) where she focuses on U.S. national security, illicit networks, transnational organized crime, and counterterrorism issues in the Americas. As a former U.S. diplomat, international banker with Goldman Sachs, U.S. foreign policy advisor under the Clinton and Bush Administrations, and professor of international security affairs at the National Defense, Georgetown, and George Washington Universities, Professor Realuyo has over two decades of international experience in the public, private, and academic sectors. She holds an M.B.A. from Harvard Business School, a M.A. from Johns Hopkins University School of Advanced International Studies (SAIS), a B.S. from Georgetown University School of Foreign Service, and a Certificate from l'Institut d'Etudes Politiques (Sciences Po) in Paris, France.

Dr. Paulette Robinson

Paulette Robinson, Ph.D. is a Senior Research Fellow at the Center for Technology and National Security Policy, Institute for National Strategic Studies, National Defense University. Before joining CTNSP in 2013, she served as the Associate Dean for Teaching and Learning and Technology for the iCollege at National Defense University. Dr. Robinson is the leader for the Federal Consortium for Virtual Worlds, a group of over 1,600 individuals from government, industry, and academia who are interested in the use of virtual worlds in government. She is co-leading a project with the U.S. Department of Agriculture to provide secure access to virtual worlds for government. Before joining the Federal Government, Dr. Robinson was the Assistant Director for Academic Support in the Office of Information Technology at the University of Maryland. She holds a Ph.D. from the University of Maryland.

Albert Sciarretta

Lieutenant Colonel (Retired) Albert A. Sciarretta is a Senior Research Fellow at the Center for Technology and National Security Policy, Institute for National Strategic Studies, National Defense University. As a Senior Research Fellow, he assesses Army science and technology (S&T) efforts; as well as broader DoD technology and analytical needs. Mr. Sciarretta is also president of CNS Technologies, Inc., for which he supports DoD efforts related to assessing advanced military technologies, developing S&T investment strategies, and designing and executing tactical through operational demonstrations and experiment. A retired U.S. Army officer, Mr. Sciarretta's service included operational assignments, instructing at the U.S. Military

Academy, acting as a technology officer on armored vehicle task forces, and serving as Assistant to the Chief Scientist, U.S. Army Materiel Command. He has dual M.S. degrees – Operations Research and Mechanical Engineering – from Stanford University and a B.S. degree in General Engineering from the U.S. Military Academy.

Hannah Snapp

Hannah Snapp interned at the Center for Technology and National Security Policy, Institute for National Strategic Studies, National Defense University during the summer of 2014 for Dr. Paulette Robinson. She is currently a senior at Ohio Wesleyan University (OWU) in Delaware, Ohio, studying international relations, Spanish, and history. Ms. Snapp is an intern for the OWU International and Off-Campus Program office (IOCP). She is also the sitting Parliamentarian for OWU Model United Nations Club. Ms. Snapp is interested in defense and security studies with a goal of working abroad after graduation.

Acknowledgments: This work was supported in part by the Office for Future Joint Force Development, J7-Joint Force Development Directorate of the U.S. Joint Chiefs of Staff.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the U.S. Government. All information and sources for this paper were drawn from unclassified materials.

Table of Contents

Shifting Human Environment:

How Trends in Human Geography Will Shape the Future Operating World

Preface

In January 2014 the Center for Technology and National Security Policy was asked to examine some major trends within the domain of human geography, developments that will have important influence on the type of environments future military forces will be operating in. Experts were identified to address the following key topics:

- Population, migration and the development of megacities
- Technology change and education
- Ideological and cultural factors in conflict
- Irregular and hybrid threats
- Growth of transnational crime organizations and activities

One goal of this effort was to provide useful information to DoD policy makers engaged in future force planning and "futures thinking." The papers contained in this volume all deal with major developments and trends in the human arena that are likely to change the way military forces must operate in the future. Each paper contains a section addressing anticipated implications for future military operations. And by presenting these papers as a package, the reader is encouraged to move beyond a simple recognition of particular trends, and consider how these factors may interact to shape a more complex and surprising future operating environment.[1]

As economic growth has spread to more and more of the developing world, an unprecedented level of migration to large urban centers has occurred in response. The first paper by Bartone and Sciarretta explores the rise of these "megacities," and what they mean for the future of U.S. defense policy. According to the United Nations, by 2025 there will be 37 megacities worldwide, up from 27 today. Up until now, the U.S. military has attempted to avoid operating in hostile urban environments whenever possible. Bartone and Sciarretta show that the military needs to develop significant urban warfare capabilities in order to effectively carry out future missions.

Albert Sciarretta's paper on ideology and decision making examines how bias shapes and informs the decisions that government and non-government groups make. Sciarretta reviews the various types of biases and ideologies that leaders have, including religious, pragmatic, and cultural beliefs systems. Understanding what these ideologies are, how they influence thought processes, and who possesses them is critical in order to develop strategies to face emerging threats.

[1]For a discussion of the perils of simple trend analysis and the value of more integrative thinking in future force planning, see Jeffrey Becker, "Contexts of future conflict and war." *Joint Force Quarterly, 74*, 15-21 (2014).

One way that future adversaries are likely to employ force is through a mix of conventional warfare, irregular tactics, weapons of mass destruction, terrorism, cyberattacks, and criminal behavior called hybrid warfare. James Keagle's paper on hybrid threats explores the nature of hybrid threats and ways in which the U.S. can counter them. Understanding the hybrid threat is critical for, as Keagle explains, hybrid threats are often located in the global commons that the U.S. has sought to control. This paper is especially timely, as Russia has employed elements of hybrid warfare in its assault on Ukraine. As more and more actors turn to the tactics associated with hybrid warfare, the U.S. military must develop capabilities and strategies to counter them.

Celina Realuyo's paper addresses the rising threat the U.S. will face from transnational criminal enterprises. New opportunities, such as cyberspace, now allow transitional criminal elements to spread their operations further and faster than before. While the globalized economy has created previously unimaginable wealth and opportunities, it has also come with a dark side. Transnational criminal groups and international terrorists have used the same infrastructure to enrich themselves and promote their interests around the world. As transnational criminal networks become wealthy, they will seek to infiltrate and corrupt government institutions, creating in effect "criminal states" that protect and promote the interests of the gangs that control them. Transnational criminal networks have also found common cause with terrorist groups, with both operating in the same "governance gaps" that permit their behavior. A renewed whole of government approach to transnational criminal gangs will be necessary in order to combat this emerging threat.

Robinson, Armbruster, and Snapp's contribution on the future of education details how changes in technology and approaches are reshaping education, not only in the U.S. but around the world. New approaches to education, such as flipped classrooms, competency based education, massive open online courses (MOOCs), and mobile learning are challenging educational institutions to rapidly adapt. In addition, advanced technology makes education more affordable and accessible to more people, and further advances are expected to radically re-order the educational landscape. Virtual classrooms, augmented reality, 3D printing, and gamification are all challenging the traditional model of education. U.S. military leaders need to understand how these changes will both impact our society and how they will affect the rest of the world.

Taken together, these papers describe an increasingly networked, technologically sophisticated and complex world that the U.S. military will have to operate in. By being aware of these trends, national security leaders and decision makers will be better equipped for the awesome task of anticipating future force challenges and requirements.

Megacities: Future Urban Environments and Joint Urban Warfare

Paul T. Bartone[1]
and
Albert A. Sciarretta

Urban operations are the most likely form of military operations facing our military forces in the future. More than half the world's population now lives in cities, and the numbers are growing every year. Additionally, the complex topography of urban areas affords significant advantages to our adversaries, since dense urban infrastructures make it difficult for U.S. forces to fully employ long-range sensors and munitions. Moreover, civilian populations are an ever-present reminder of the need to avoid collateral damage. These issues associated with urban operations escalate tremendously when they must be conducted in a megacity. A megacity is one which has a population of 10 million or more. There are currently over 20 megacities in the world, and the number is growing rapidly. How should U.S. military forces be configured and equipped to function effectively in such environments? This brief concept paper addresses the rapid growth of "megacities" and the implications for future security and urban operations.

Population Trends

Several major population and demographic trend were recently identified by Professor Mark Haas of Duquesne University.[2] These are:

- High population growth in developing countries
- Massive population aging in developed countries
- Continued youth bulges in Africa and Middle East
- Growing gender imbalances in Asia and Europe
- Declining fertility in all regions

Strikingly, 98 percent of the world's population growth from now to 2050 is expected to occur in developing countries, mostly in Africa, as well as India, Pakistan, and the Philippines. With the notable exception of the United States, most of the world's developed countries are expected to decline in population. In addition, declining fertility rates in the developed world, along with the aging of previous "baby boom" generations, is going to mean increasing older populations. Figure 1 shows the median age increase in seven major world countries over a 100-year period.

[1] bartonep@gmail.com
[2] Information in this section draws upon material presented by Mark Haas at the J7 Futures Human Geography Seminar. Johns Hopkins Applied Physics Laboratory, Laurel, Maryland, June 18, 2014.

Figure 1. Median Population Age in Major World Powers, 1950 to 2050

Country	1950	2000	2050
United States	30.0	35.3	40
France	34.5	37.7	42.7
United Kingdom	34.9	37.7	42.9
Russia	25.0	36.5	43.1
China	23.8	29.7	48.7
Germany	35.4	39.9	49.2
Japan	22.3	41.3	52.3

Source: United Nations World Population Prospects (http://esa.un.org/wpp/unpp/panel_indicators.htm) as summarized by Mark Haas, J7 Human Geography Seminar, June 8, 2014. Cited with permission.

Looking just at the period from 2000 to 2050, the most dramatic increase is occurring in China, where median age will increase by almost 20 years from 29.7 to 48.7. Germany, Japan, and Russia will increase by nearly 10 years, and the United Kingdom, France, and the United States by about 5 years. This will mean a smaller working age population in these countries, likely declines in gross domestic product, and growing government spending on providing support and care for the elderly. This trend will also create increasing pressure to decrease defense budgets in the affected countries. One implication for the United States is that traditional allies will be less likely to step forward and share the burden of military operations when called upon. In defending its strategic interests, the United States may have to act unilaterally to a greater degree than desired.

The Growth of Megacities

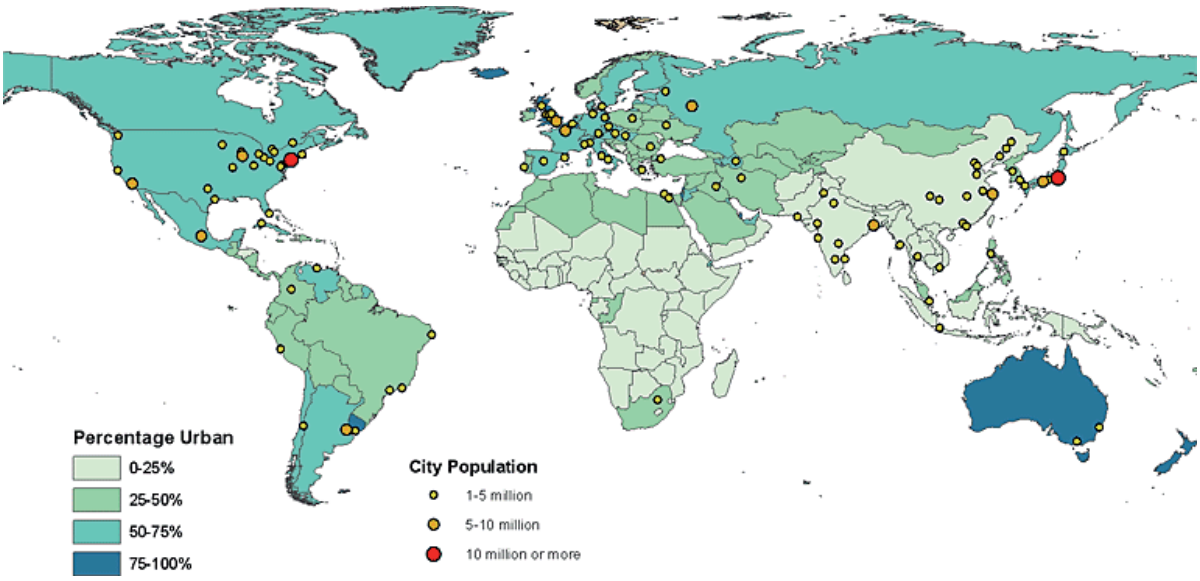
Massive population growth in the developing world is coupled with increasing migration of people to urban environments. Across the globe, people are moving to cities in ever larger numbers. Many factors account for this trend, including better perceived economic opportunities in cities, declining job and farming prospects in rural areas, conflict and strife pushing people to seek safety in cities, and better health and education services.[3] While this trend is apparent in cities of all sizes, the most rapid population growth is seen in what have been called "megacities." Figures 2 and 3 graphically display the growth trend in world urban population from 1960 to 2025. Cities with 1 to 5 million people are shown as small yellow dots, 5 to 10 million people as larger orange dots, and cities with greater than 10 million people as large red dots.

The United Nations (UN) has somewhat arbitrarily defined a megacity as having a population over 10 million. In 1970, by this definition, there were two megacities in the world. By 2011,

[3] As discussed in presentation by Peter Engelke, Migration and Urbanization: Overview and Implications. J7 Futures Human Geography Seminar. Johns Hopkins Applied Physics Laboratory, Laurel, Maryland, June 18, 2014. Cited by permission.

there were 23.[4] Today, there are 27.[5] Projections are for 37 megacities worldwide by 2025.[6] Today, more than half the world's population lives in cities. By 2030, it is expected that two-thirds of the world's population will be living in cities, increasing to three-quarters by 2050.[7] Megacities such as New York, London, and Tokyo have the resources, infrastructure, and systems to provide for the needs of their residents. However, most of the new megacities are in the developing world, with large numbers of poor, and have inadequate resources, infrastructure, and systems to support this growth. These sprawling metropolises are unable to keep up with their massive numbers of people, are chaotic and dangerous, and have limited or no basic services for health and education. Often they lack any semblance of effective government.[8] As this urban growth continues and accelerates, the competition for food, water, and energy resources will also grow more acute.

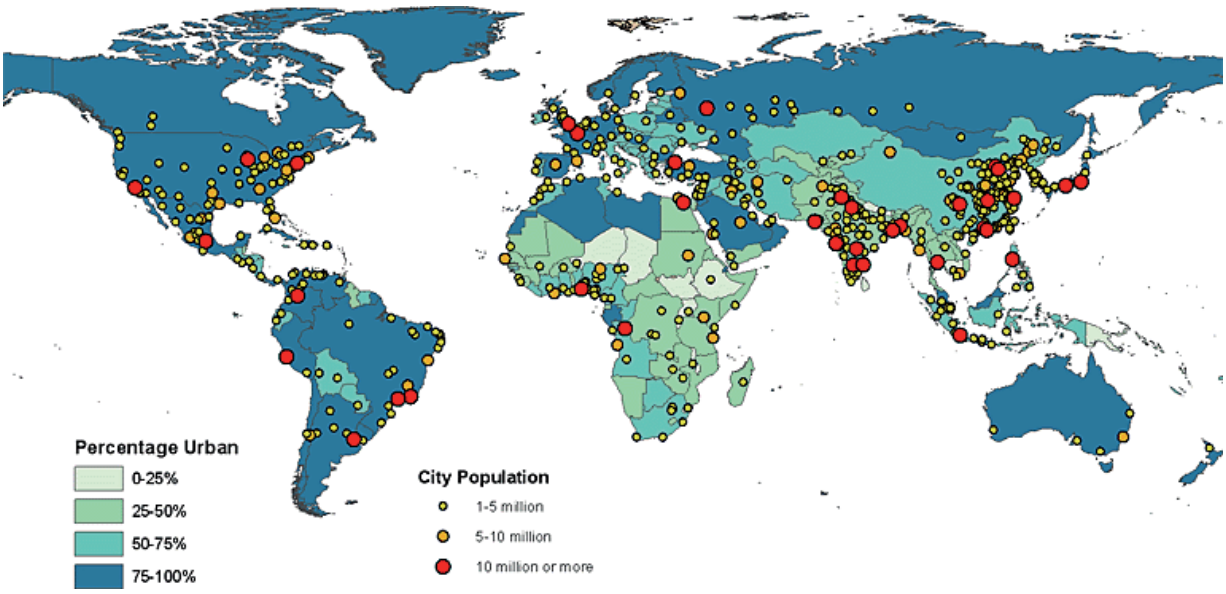
Figure 2. Global Urbanization, 1960



Source: United Nations Department of Economic and Social Affairs http://esa.un.org/unup/Maps/maps_urban_1960.htm As presented by Peter Engelke at the June 18, 2014, Human Geography Seminar. Cited with permission.

[4] United Nations, Department of Economic and Social Affairs. *World Urbanization Prospects, 2011*. New York: United Nations; 2012.
[5] Imhoff M., Brandenberger J., Calvin K., et al. Evaluating Long-term Threats to Environmental Security via Integrated Assessment Modeling of Changes in Climate, Population, Land Use, Energy and Policy. *Understanding Megacities with the Reconnaissance, Surveillance, and Intelligence Paradigm*, ed. Ehlschlaeger C. U.S. Army Engineer Research Development Center, Topical Strategic Multilayer Assessment. Available at www.kalevleetaru.com/Publish/Understanding-Megacities-Reconnaissance-Surveillance-Intelligence.pdf
[6] United Nations, Department of Economic and Social Affairs.
[7] For a summary of these trends, see Kilcullen D. *Out of the Mountains: The Coming of Age of the Urban Guerrilla* Oxford: Oxford University Press; 2013: 27–31.
[8] Liotta P.H., Miskel J.F., *The Real Population Bomb*. Washington, DC: Potomac Books; 2012.

Figure 3. Global Urbanization, 2025



Source: United Nations Department of Economic and Social Affairs http://esa.un.org/unup/Maps/maps_urban_2025.htm . As presented by Peter Engelke at the June 18, 2014, Human Geography Seminar. Cited with permission.

As more of the world's population becomes concentrated in the sprawling urban environments of megacities, scarcities of food, water, and energy will lead to increased competition and conflict. Natural disasters such as earthquakes will continue to occur, and their impact may be greater as people are more concentrated in space. It is also the case that most megacities are located close to coastal areas, making them more vulnerable to tsunamis, typhoons, high winds, hurricanes, and flooding. Climate change can be expected to bring even more disruption. For example, a recent report by the National Research Council concludes that we know "beyond a reasonable doubt" that the consequences of climate change will be extensive.[9] The report states that "*given the available scientific knowledge of the climate system, it is prudent . . . to expect climate surprises in the coming decade, including unexpected and disruptive single events as well as conjunctions of events occurring simultaneously or in sequence, and for them to become more serious and more frequent thereafter.*" With sea levels projected to rise due to global warming, littoral megacities are even more vulnerable to such disasters and flooding than inland cities are.[10]

The destructive impact of natural disasters will also be greater in megacities, and disaster response will be more difficult. Infectious diseases will also be more difficult to control in megacities where people are crowded together and sanitation and healthcare services are already weak or nonexistent. In megacities, the containment of deadly viruses, such as Ebola, becomes

[9] National Research Council. Committee on Assessing the Impacts of Climate Change on Social and Political Stresses. *Climate and Social Stress: Implications for Security Analysis.* Washington, DC: The National Academies Press; 2012.
[10] World Bank, Independent Evaluation Group. Development Actions and the Rising Incidence of Natural Disasters. Washington, DC. http://ieg.worldbankgroup.org/Data/reports/developing_actions.pdf

almost impossible, as seen in the nightmare now being experienced in Freetown, Sierra Leone, or Monrovia, Liberia. All of this is a recipe for increased competition and conflict. Criminal groups, gangs, and cartels operating in megacities further increase the potential for violence and conflict. Megacities provide extensive cover for such groups, making law enforcement more difficult. The same is true for many radical ideological and religious groups, which increasingly will operate, plan, and train within the environment of megacities. The challenges and problems presented by future megacities go beyond what the military can address, of course, and will have to be confronted by all segments of the U.S. Government. The core role of the military is to provide force when necessary to protect national interests and security. While military operations have historically occurred mostly in open rural environments, in the future, demographic and urbanization trends dictate that military forces will have to operate much more frequently in the messy urban environment of megacities, against adversaries who will use asymmetric or irregular methods.[11]

As Kilcullen points out, these megacities are also characterized by dramatically increased levels of electronic connectedness, through the Internet, cell phones, and broadcast media.[12] Even areas that are desperately poor and lacking in many basic services often have good access to the Internet, cell phones, radio, and television. For example, in the collapsed state of Somalia, as of 2011 over 25 percent of the Somalian people were using cell phones.[13] These communications technologies are being applied by groups on all sides of conflicts to increase awareness of what is happening in areas of operations, to share information, and to coordinate their actions. Communications technologies also make it possible for remotely located command groups to provide attacking forces with real-time information regarding developments around them, and minute-to-minute instructions on how to proceed. This is exactly what happened, for example, in the 2008 terror strikes in Mumbai, in which 10 attackers killed 172 people and wounded 304. The attacks were managed by a remote command cell in Karachi, Pakistan.[14]

Implications for Future Military Operations

Given that future military operations are more likely to occur in the urbanized, highly crowded, and riverine environments of littoral megacities, what are the implications for future military forces? The United States has proven its combat superiority on open terrain. However, many would argue that we do not have equivalent superiority in urban environments. This is not because American warfighters are less capable, but because our training, doctrine/tactics, and operational technologies do not provide the same advantages they provide in open, rolling terrain. The U.S. investment in large mechanized forces and air-to-ground engagement systems has provided military superiority in rural environments, but that investment does not address the complex urban environment, especially when constrained by rules of engagement that seek to minimize collateral damage. In an attempt to offset U.S. advantages in open terrain, adversaries often move the confrontation to the urban environment. To minimize civilian casualties and

[11] Kilcullen.
[12] Ibid., 32–37.
[13] Gagliardone I., Stremlau N., *Digital Media, Conflict and Diasporas in the Horn of Africa.* London: Mapping Digital Media Program of the Open Society Foundations; 2011: 9–10.
[14] Roy N., Kapil V., Subbarao I., and Ashkenazi I., Mass Casualty Response in the 2008 Mumbai Terrorist Attacks. *Disaster Management and Public Health Preparedness,* 5. 2011: 273–279.

collateral damage, U.S. commanders often choose to avoid battle in large urban areas. Our adversaries, however, have no such qualms about endangering noncombatants. Additionally, many of our strategic and operational command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems are often less effective in urban environments. Dense, complex structures and civilian populations make it harder to discern the enemy. U.S. urban doctrine for large complex cities is less tested, and our joint urban training is less well-developed. Current tactics and military equipment call for our military to enter a building mostly on the first floor (through doors and windows) or on the roof (using helicopters) and force the use of stairwells to move from floor to floor. Our enemies know this and will be able to design their defenses to exploit this limitation. The performance of U.S. warfighting systems will be severely limited in megacity environments. For example, huge buildings will block global positioning system (GPS) signals internally and degrade them externally, which will limit the use of precision-guided munitions, GPS-guided robotic systems, and GPS-based Blue Force Tracking systems. While the United States does not "lose" these battles, they reduce the nature of the fight to a war of attrition, which is a disadvantage to American forces.

Kilcullen provides an insightful and well-documented analysis of the implications of these developments for future military forces.[15] By his account, there is a clear need for Marine and Special Operations amphibious forces, highly maneuverable Navy supply ships, and expeditionary logistics. Also important are rotary-winged aircraft that can move people and equipment quickly, as well as precision weapons and targeting systems that can operate in GPS-degraded environments and reduce collateral damage. Combat engineers and civil affairs units will be needed for many construction and rebuilding activities. Forces will need to be organized such that they can be rapidly reconfigured into smaller elements that can operate independently. Also, forces should be self-sufficient as much as possible with respect to food, water, and other essential supplies. C4ISR systems that can operate in noisy environments with extensive background clutter will be needed, as will sensor systems to provide early warning and delineation of problem areas.

With respect to C4ISR systems, having small units (company through squad) integrated into the larger Service and joint networks is essential, especially Blue Force Tracking down to the individual warrior. Without this C4ISR integration in large, complex, joint urban operations, the probability of fratricide will be high.

For all Services, more education and training time should be devoted to understanding the future operating environment of megacities, and littoral megacities in particular. The more we understand these complex environments, the better prepared we will be to conduct a range of operations within them. As F.G. Hoffman and G.P. Garrett have recently argued, preparing future military forces to operate effectively in these environments will necessitate a longer training and education pipeline, in order to acquire the needed culture and language skills as well as urban combat skills.[16] Further, joint military education at all levels should incorporate the study of megacities, to include geographic, social, cultural, economic, and political aspects. Case

[15] Kilcullen.
[16] Hoffman F.G., Garrett G.P., *Envisioning Strategic Options: Comparing Alternative Marine Corps Structures.* Washington, DC: Center for a New American Security; 2014: 13. http://www.cnas.org/sites/default/files/publications-pdf/CNAS_MarineCorps_HoffmanGarrett.pdf

studies of megacity environments would be very beneficial in this regard and could include, for example, Mumbai (India), Jakarta (Indonesia), Lagos (Nigeria), Guangzhou (China), Karachi (Pakistan), Dhaka (Bangladesh), Mexico City (Mexico), and Sao Paulo (Brazil).

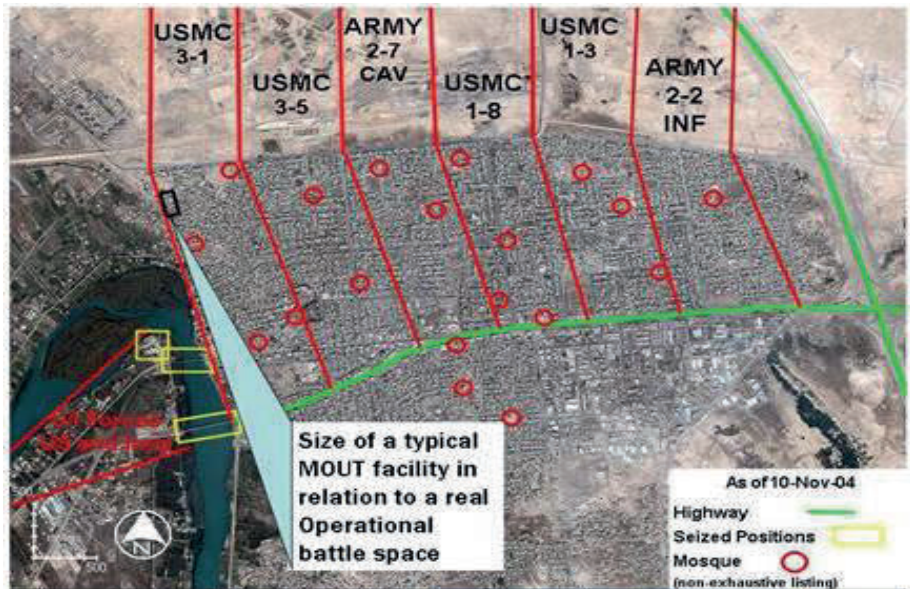
Practical training to prepare forces for operating in megacity environments also merits greater emphasis. A 2006 report by the Defense Science Board indicated a pressing need for more realistic training facilities to train joint forces to operate in urban environments, with "*urban training environments (physical, infrastructure, cultural, adversarial) large enough to 'swallow' a battalion.*"[17] Unfortunately, this advice has not been heeded. Today, there are still no facilities available to adequately train a joint force operation in a large city. As an example, consider Operation *Al Fajr* (Arabic for "New Dawn") in Fallujah, Iraq. An estimated 10,000–15,000 American troops launched Operation *Al Fajr* in Fallujah on November 8, 2004. This followed weeks of aerial bombardment by U.S. planes. A number of trained Iraqi forces also participated in the operation. Figure 4 shows the city of Fallujah, the U.S. military units participating in Operation *Al Fajr*, and the size of their operational sectors. Note the small black rectangular box in the upper left corner of the city. This depicts the size of a typical Military Operations on Urban Terrain (MOUT) training facility in the United States.

There are numerous such MOUT training facilities in the United States, with one located at almost every military base. However, as Figure 4 makes clear, these are all quite small, and do not realistically represent the challenges of typical, let alone megacity, urban operations. The largest U.S. urban training facilities are found at the Muscatatuck Urban Training Center (MUTC) and the Joint Readiness Training Center (JRTC). However, even these somewhat larger MOUT facilities are lacking in realism, without a local population, transportation infrastructure, communications, utilities, radio signals, commerce systems, and other aspects of a living, breathing city. These training areas are insufficient to provide the operational realism and technical relevance required to evaluate a battalion-size urban operation while experiencing the aggregate effects provided by a realistic urban environment. This is an especially important issue for testing the performance of joint weapons and C4ISR systems in modern urban environments.[18]

[17] Defense Science Board Task Force, Force Protection in Urban and Unconventional Environments. (March 2006) Defense Technical Information Center Accession Number ADA446191. www.dtic.mil/docs/citations/ADA446191 and www.dtic.mil/get-tr-doc/pdf?AD=ADA446191

[18] Report on Joint Operations on Urban Synthetic Terrain Experiment. Defense Modeling and Simulation Office. (November 2004), https://sw.csiac.org/techs/abstract/548655

Figure 4. Comparison of a typical MOUT facility to the size of Operation Al Fajr



[19]

Source: Report on Joint Operations on Urban Synthetic Terrain experiment, Defense Modeling and Simulation Office, November 2004, abstract available at https://sw.csiac.org/techs/abstract/548655

More investment is needed in building realistic training and testing facilities for individual military service and joint operations. Battalion-size and larger "physical" facilities for training and testing are not necessarily needed. Perhaps the distributed integration of existing physical facilities with augmentation from computer-based and virtual training/testing facilities would provide a better approach. There is also a need for greater Navy and Air Force participation in urban warfare training facilities and exercises. The 2006 Defense Science Board report recommended that the Joint Urban Operations Activity (JUOA) at U.S. Joint Forces Command (JFCOM) focus its efforts on orchestrating more Service contributions to urban operations and take the lead in sponsoring a few major joint urban training exercises each year.[20] Since JFCOM was disestablished in 2011 in a cost-cutting move, it is not clear if anyone in the Department of Defense has taken up the important role of JUOA. Some of the advances in educational technologies described by Robinson, Armbruster and Snapp (2015, this volume) could be applied in this context to provide cost-effective training and education for Urban Operations Activity. Advanced educational technologies, combined with realistic training facilities, could give us a relatively low-cost yet effective learning environment.

There are also implications for joint doctrine. Operations in littoral urban environments are not covered in current doctrine—for example, in the joint publication on amphibious operations[21] or

[19] Army Test and Evaluation Command proposal for Joint Urban Operations Integrated Live-Virtual-Constructive Tactical-to-Operational Test and Training Capability (JILT3C) Program. February 2007: 3
[20] Defense Science Board Task Force. 42–43. 1
[21] U.S. Department of Defense. Joint Publication 3-02. *Amphibious Operations.* Washington, DC: Department of Defense; 2009.

in joint doctrine for forcible entry operations.[22] In contrast, the U.S. Marine Corps has given considerable attention to complex operations in urban littoral environments in its own operations doctrine.[23] Joint forces doctrinal publications, as well as those of the Army and Air Force, need to be updated to include operations in the expected future operating environment of huge and complex coastal cities.

If operations in complex urban environments are more likely in the future joint operating environment, consideration must also be paid to force structure and basing. For the U.S. Marine Corps, Hoffman and Garrett recommend a hybrid structure that preserves the capability to respond rapidly to major regional threats (for example, China) with sustainable force projection, while also providing expanded capacity to deal with small conflicts in urban environments.[24] Under this proposal, four Marine Expeditionary Brigades would be based regionally, with one in the Western Pacific, one in the Mediterranean, and one on each coast of the continental United States. Approximately half of Marine battalions would be specialized for operations in the littoral, urban environment of megacities, as would the Marine Forces Reserve. These units would also regularly rotate into Special Operations units for joint training and support.

While it is difficult to predict the future, the demographic trends are clearly leading to a world dominated by sprawling, crowded, and chaotic megacities, often with poor resources, weak governance, and a high potential for conflict. The U.S. Marine Corps is leading in efforts to prepare for such a future operating environment. The other Services and the entire Joint Force would be wise to do the same.

[22] U.S. Department of Defense. Joint Publication 3-18. *Joint Forcible Entry Operations.* Washington, DC: Department of Defense; 2012.
[23] United States Marine Corps. MCDP 1-0. *Marine Corps Operations.* Washington, DC: Headquarters, U.S. Marine Corps; 2001.
[24] Hoffman and Garrett. 12–17.

References

Becker J. (2014). Contexts of future conflict and war. *Joint Force Quarterly, 74*, 15-21.

Defense Modeling and Simulation Office. *Joint Operations on Urban Synthetic Terrain.* November 2004. https://sw.csiac.org/techs/abstract/548655.

Defense Science Board Task Force. *Force Protection in Urban and Unconventional Environments*. Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, DC, March 2006. www.dtic.mil/get-tr-doc/pdf?AD=ADA446191.

Gagliardone I., and Stremlau N. (2011). *Digital Media, Conflict and Diasporas in the Horn of Africa.* London: Mapping Digital Media Program of the Open Society Foundations.

Hoffman F.G., and Garrett G.P. (2014). *Envisioning Strategic Options: Comparing Alternative Marine Corps Structures*. Washington DC: Center for a New American Security.

Imhoff M., Brandenberger J., Calvin K. et al. (2014). "Evaluating Long-term Threats to Environmental Security via Integrated Assessment Modeling of Changes in Climate, Population, Land Use, Energy and Policy." In C. Ehlschlaeger, ed., *Understanding Megacities with the Reconnaissance, Surveillance, and Intelligence Paradigm*. U.S. Army Engineer Research Development Center, Topical Strategic Multilayer Assessment. www.kalevleetaru.com/Publish/Understanding-Megacities-Reconnaissance-Surveillance-Intelligence.pdf.

Independent Research Group (2007). *Development Actions and the Rising Incidence of Natural Disasters.* Washington, DC: World Bank. http://ieg.worldbankgroup.org/Data/reports/developing_actions.pdf.

Kilcullen D., (2013). *Out of the Mountains: The Coming of Age of the Urban Guerrilla*. Oxford: Oxford University Press.

Liotta P.H., and Miskel J.F. (2012). *The Real Population Bomb*. Washington, DC: Potomac Books.

National Research Council. (2012). *Climate and Social Stress: Implications for Security Analysis.* Committee on Assessing the Impacts of Climate Change on Social and Political Stresses. Washington, DC: The National Academies Press.

Roy N., Kapil V., Subbarao I., and I. Ashkenazi. (2011). "Mass Casualty Response in the 2008 Mumbai Terrorist Attacks." *Disaster Management & Public Health Preparedness* 5, 273–279.

United Nations (2012). *World Urbanization Prospects, 2011*. New York: UN Department of Economic and Social Affairs.

U.S. Department of Defense (2009). Joint Publication 3-02, *Amphibious Operations*. Washington, DC: Department of Defense.

——— (2012). Joint Publication 3-18, *Joint Forcible Entry Operations.* Washington, DC: Department of Defense.

United States Marine Corps (2001). Marine Corps Doctrinal Publication 1-0, *Marine Corps Operations*. Washington, DC: Headquarters, U.S. Marine Corps.

Identity and Ideological Conflict: Influences of Religious, Cultural, and Pragmatic Ideologies on Political Groups

Albert A. Sciarretta[1]

Importance of Ideology

Terrorist attacks are often described as being "indiscriminate," implying that random violence is committed with little thought as to who or what is harmed. In practice, however, attacks by terrorist groups are rarely indiscriminate. Instead, target selection is determined by a number of factors, but mostly ideology – a set of ideas and beliefs of a group or political party.[2] While ideology is not the only factor that determines whether a potential target is attacked, it provides an initial range of legitimate targets and a means by which terrorists seek to justify attacks, both to the outside world and to themselves. As an example of a factor other than ideology, terrorists may focus on the effects of an attack and the resultant publicity.

Ideology plays an important role in the decision-making processes of governmental and non-governmental (e.g., terrorist organization) political groups. Ideology can provide an initial motive or justification for a decision or action. It can also act as a lens, albeit biased, through which a political group can view events and the actions of other people. Most individuals and political groups are motivated by an ideology, unless they are motivated purely by a desire for power and the benefits that come with it.

This perception of the importance of ideology in planning and decision-making processes is validated in 1998 by C. J. M. Drake.[3] The author evaluated numerous Western European terrorism case studies to surmise that ideology "*provides terrorists with the moral and political vision that inspires their violence, shapes the way in which they see the world, and defines how they judge the actions of people and institution.*" Drake further states that ideology "*allows the terrorists to dehumanise those people whom they intend to harm – seeing them as symbols rather than as flesh and blood human beings.*"

More recently, Austin L. Wright endorsed the importance of ideology.[4] He developed a theoretical and empirical model, using data on Western European terrorism from 1965 to 2005. In his model-based analysis, he determined that ideology is the only consistent predictor of target selection by terrorists, even when other relevant strategic considerations are present. His results were particularly robust for nationalist-separatist groups and religious groups.

---

[1] asciarretta@cnsti.com

[2] Ideology. Merriam-Webster, n.d. (16 Sept. 2014) http://www.merriam-webster.com/dictionary/ideology

[3] Drake C. J. M., The Role of Ideology in Terrorists' Target Selection. *Terrorism and Political Violence Vol. 10*. No. 2; 1998: 53-85

[4] Wright A.L., Terrorism, Ideology and Target Selection. Department of Politics, Princeton University. Version 1.1, March 5, 2013.

Identifying Ideological Biases

The understanding of ideological biases of people can be helpful in understanding the planning and decision-making processes of political groups, especially if the biases of predominant members are known. Political groups may exhibit a number of biases. The discussion in this paper will focus on three basic ideological biases: religious (e.g., Shia Islam, Christianity), pragmatic (e.g., survival, national security, balance of power), and cultural (e.g., Arab culture, Western culture). Each member of an ideological group will have elements of all three biases – and maybe others – and each will most likely have a dominant perspective that greatly influences planning and decision-making processes of that person, as illustrated in Figure 1. Terrorism and counterterrorism academicians and operators developed this concept of depicting the predominance of ideological biases during a Combatting Terrorism Technical Support Office (CTTSO) Technical Support Working Group (TSWG) counterterrorism research project conducted in 2005-2006. A majority of the operators had personal knowledge of terrorist cells operating in the Middle East region.

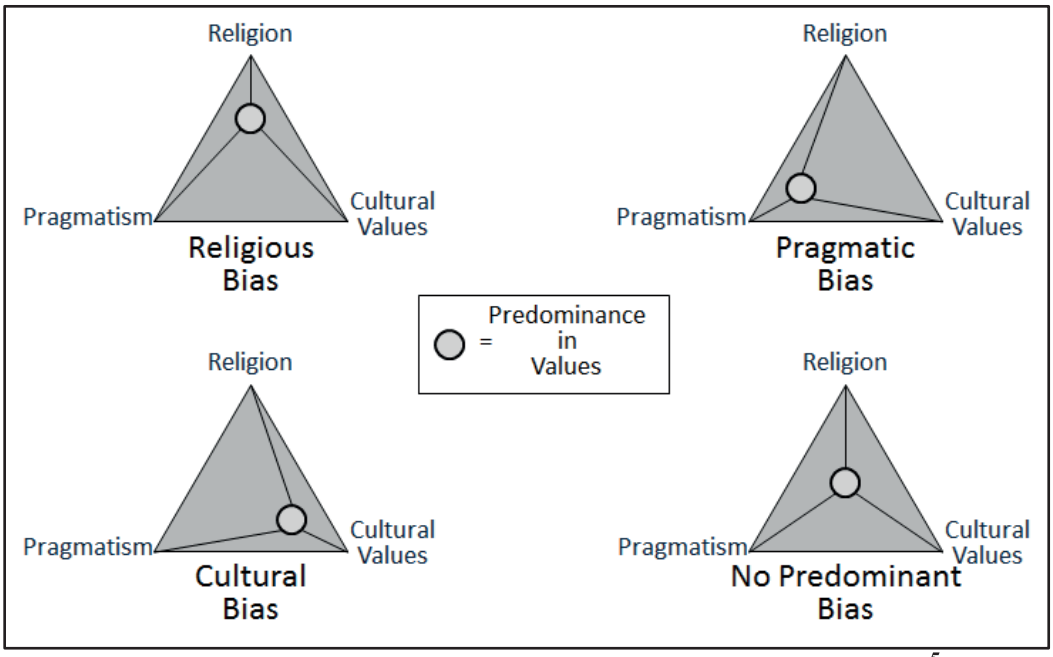


Figure 1. Depicting the Predominance of an Ideological Bias[5]

Religious Bias

A person with a religious, or faith-based, bias may try to convince others to plan and make peaceful or violent decisions based on the teachings of a religion. For example, a person of Islamic faith may make references from the Quran and Islamic history to make specific points for convincing others that their actions were consistent or inconsistent with Shia Islam. The word

[5] Conceptual drawing developed during CTTSO/TSWG counterterrorism research project, 2005-2006. For details, contact CTTSO/TSWG office. For information on CTTSO, see http://www.cttso.gov/ .

jihad – a term often used to represent a religious struggle – is cited numerous times in the Quran. A non-violent religious person may use the Quran's term jihad to support a non-violent inner religious struggle, in addition to the Quran's opposition to killing innocent people. A person supporting violence may use the interpretation that jihad is an armed struggle against those who attempt to persecute or oppress Islam.

Similarly, religious biases may be seen in a person of Christian faith. In the Middle Ages, the Roman Catholic religion sanctioned the Crusades to secure Christian access to the Holy Land. Today, the "Christian right" (i.e., religious right) in the United States may support political decisions resulting in socially conservative policies. Just as the word jihad in the Quran can be used for peace or violence, so too can words in the Bible be used for peace (e.g., "*...whoever slaps you on your right cheek, turn the other to him also.*"[6]) or for violence (e.g., text related to "an eye for an eye"[7]).

Pragmatic Bias

People who are strongly pragmatic, concerned about their country, host country, region, tribe, or terrorist organization, may argue that self-survival and loyalty are most important to the group's decision. For example, a pragmatic leader of the Taliban – an Islamic fundamentalist political movement in Afghanistan, with diplomatic recognition in Pakistan – would oppose decisions that might result in political, economic, or military retaliation against the Taliban or Pakistan.

Pragmatic bias has played a significant role in justifying major conflicts. Prior to World War II, Germany wanted to counter the Treaty of Versailles by restoring the boundaries of historic Germany, as well as reinvigorating national pride. Similarly, Japan needed to expand its boundaries because of its lack of vital natural resources. Today, Russia has cited similar justifications for its actions in Crimea and the Ukraine.

Cultural Bias

Eikelman states: "*Culture refers generally to a set of implicit, widely shared assumptions about how things work in a society and how they ought to work – at least for one's group of reference.*"[8] A person with strong cultural values may use ideas of honor, revenge, retaliation, and shame to coax members of a group to take actions that would resonate with, for example, the Arab world. This use of culture to influence decision-making processes is reinforced by Briley's[9] description of how culture affects decision-making processes. For instance, Briley believes that European Americans are generally influenced by the positive consequences of a decision, whereas Asians appear to be more influenced by the negative consequences that may occur due to a decision or line of action. Cultural biases may also support illicit activities such as corruption and use of drug sales to finance activities.

---

[6] New American Standard Bible. Matthew 5:39
[7] New American Standard Bible. Exodus 21:23-21:25
[8] Eickelman D.F., Culture and Identity in the Middle East: How They Influence Governance. *Fighting Chance: Global Trends and Shocks in the National Security Environment.* Washington, DC: Center for Technology and National Security Policy, National Defense University, Potomac Books, Inc.; July 2009: 160.
[9] Briley D., Reasons as Carriers of Culture: Dynamic versus Dispositional Models of Cultural Influence on Decision Making. *Journal of Consumer Research (JCR).* Vol. 27; September 2000.

No Predominant Bias

A person or group with no predominant bias may place equal importance on religion, pragmatism, and culture – siding with the person who has the strongest religious, pragmatic, or cultural arguments. These individuals may also disregard all three ideologies and consider self-interests as being most important. The desire for power and the benefits that come with it may significantly outweigh the importance of any ideology.

Additional Ideologies and Unclear Ideological Biases

This paper focuses on three ideological types or biases – religious, pragmatic, and cultural – for several reasons. First, space limitations prevent a detailed study of many different ideologies. For example, terms such as political, social, ethical, and philosophical could be substituted for or included as additional terms in the above analysis. Second, the author's experience in counterterrorism research[10] has revealed that religious, pragmatic, and cultural biases worked quite well for the analysis of terrorist organizations in the Middle East.

Decisions can be significantly influenced by one's past and/or current experiences – both ideological and non-ideological. This *experiential bias* may significantly augment or even alter ideological biases, affecting decision-making processes much more than any particular ideology. Preconceived notions developed while growing up, by watching television (especially American television), by viewing Web sites (especially propaganda Web sites), or by interacting with others on social media networks may have a huge impact on how an individual or ideological group perceives the need for or potential outcome of an action.[11]

In addition to identifying appropriate ideologies, it is important to recognize when ideologies might overlap, making it difficult to define a predominant ideology for an individual or group. For example, it is difficult to clearly define Islam as a religious or political (e.g., democracy, communism, socialism) ideology. It is a religion in the same context and group as Christianity, Judaism, Buddhism, among others. However, one could also consider Islam in the context of political/social structures such as socialism, communism, and democracy.[12] Islamic religious leaders are deeply involved with governments, militias, and armies throughout the Middle East. Examples of religious involvement with politics are the identification of religious leaders as political leaders (e.g., Supreme Leader of Iran[13]), the use of Islamic law (shariah) as the law of the land, and the banning of any speech deemed anti-Islam by Muslims. In addition, religion may create political linkages among nations. In Muslim countries, Iran, Iraq, and Azerbaijan might be more closely aligned because of the preponderance of Shia Islam in those countries, while other

[10] Participation in a Combatting Terrorism Technical Support Office (CTTSO) Technical Support Working Group (TSWG) counterterrorism research project, 2005-2006. Thrust of the effort was to use highly experienced counterterrorism experts to simulate the planning of a terrorist attack, and observe their thought processes.
[11] Technical discussions with Michael Hopmeier, President, Unconventional Concepts, Inc., 7 May 2014 [Note: Mr. Hopmeier also participated in the CTTSO/TSWG counterterrorism research project, 2005-2006]
[12] CTTSO/TSWG counterterrorism research project, 2005-2006.
[13] The Supreme Leader of Iran is the head of state and highest ranking political and religious authority in the Islamic Republic of Iran.

Muslim countries might be aligned because of the dominance of Sunni Islam. Thus, Islam could be considered a "political religion."

Religion may also overlap with culture. A religion may be as important as ethnicity – being Islamic may be just as important as being an Arab. In the case of Islamic religion and culture, they are closely intertwined. For example, a traditional interpretation of Islam may be used to prevent girls from attending school. However, in many other cases, culture is much more than religion and many cultures include multiple religions – as in "American culture" in the United States. In addition, throughout history, religions have split, creating splinter groups, each with its own beliefs and culture. It is no different in the Muslim world with Shiite and Sunni Muslims.

As a final example, consider the motivations of Islamic suicide bombers. Is the bomber taking his life because of a specific ideology: religious (oppose those who oppose Islam), pragmatic (loyalty to or survival of his family), or cultural (retaliation for actions against his tribe)? Or, is he merely seeking personal rewards in terms of money/care for his surviving family, personal fame, or the perceived belief of having access to 72 virgins in Paradise?[14] Recent events have shown that a female suicide bomber may take her life to offset the personal shame associated with being raped. This notion has been used by terrorists to convert vulnerable women into suicide attackers. The mode of operation is to identify a woman, lure her somewhere to be raped, and then tell her that her only option for salvation is to become a suicide bomber.[15]

Implications for Future Military Operations

As described above, ideological biases can be used by individuals to persuade others and eventually come up with a plan or decision for which all members of a group agree. The understanding and manipulation of this dynamic can be extremely beneficial to U.S. decision makers. Once ideological biases of an individual or group are known, intervention techniques might be used to manipulate the biases and make ideological opponents undertake actions that are ultimately in the interest of the United States.

For example, a terrorist organization with dominantly pragmatic values would likely be interested in political and organizational survivability following attacks against Western targets. In order to preserve this interest, the terrorists might formulate a strategy that includes carrying out attacks against the United States with a degree of deniability to avoid pushing the United States into retaliating heavily against the terrorist organization and invading its host country. It may be assumed that eventually, a U.S. investigation will present clear proof that a terrorist organization was involved in the attack. Thus, following the attack, there will be a finite amount of time available for the terrorist organization to use an information operations campaign to influence various international elements to restrain the United States from retaliating. These activities might focus on both allies of the United States as well as allies of the terrorist organization. The latter effort might create enough of a potential threat to deter the United States

[14] There is little agreement about the origin of "72 virgins in Paradise." It may be an interpretation of a apocryphal passage of the Hadith, which indicates how Muslim men will be rewarded in Paradise (i.e., wed to these virgins). Putting aside its origin, it has become a popular belief as a reward for suicide bombers.
[15] Iraq's Female Bomb Recruiter. *BBC News*. February 4, 2009. http://news.bbc.co.uk/2/hi/middle_east/7869570.stm

from attacking. Knowing all of this, U.S. decision makers might want to significantly reduce the investigation time to identify the attacker(s), quickly launch a counter-information operations campaign, quickly strengthen ties with U.S. allies, and ensure that political and/or military retaliation is taken in a timely manner.

Similar actions should be considered for terrorist organizations that have predominantly religious or cultural biases. For religious biases, alliances with senior leaders of many religions may be helpful. Likewise, cultural leaders should be sought to speak up against terrorist organizations with predominantly cultural biases. For example, emphasis on the immorality of killing innocent women and children could have an influence on both biases.

What Will Change in 2030?

The importance of ideological biases in future decision making will have little to no change, just as we have seen the importance of ideology-based wars throughout history and especially today. What may change is the manipulation of an ideology, as seen in the terrorists' targeting of vulnerable women and converting them into suicide bombers.

Conclusions

Effective planning and actions by U.S. decision makers must include the ideological biases of perceived opponents. More effort must go into identifying the ideological biases of individuals as well as those shared by groups. The importance of ideological biases has not changed much historically, and it will continue to remain important in the future. It is increasingly important for military decision makers to view the actions of perceived opponents from the perspective of their ideologies.

References

Briley D., (2000). Reasons as Carriers of Culture: Dynamic versus Dispositional Models of Cultural Influence on Decision Making. *Journal of Consumer Research (JCR). Vol 27*.

Combatting Terrorism Technical Support Office (CTTSO) Technical Support Working Group (TSWG) counterterrorism research project. (2005-2006). For details, contact CTTSO/TSWG. For information on CTTSO, see http://www.cttso.gov/.

Drake C. J. M., (1998) The Role of Ideology in Terrorists' Target Selection. *Terrorism and Political Violence.* Vol 10. Number 2. 53-85.

Eickelman D.F., (2009) Culture and Identity in the Middle East: How They Influence Governance. *Fighting Chance: Global Trends and Shocks in the National Security Environment.* Center for Technology and National Security Policy. National Defense University. Washington, DC: Potomac Books, Inc. 157-172.

Hopmeier M., (2014) Technical Discussions. [Note: Mr. Hopmeier also participated in the CTTSO/TSWG counterterrorism research project, 2005-2006].

Malinowski J., (2014) Identity and Ideology. Presentation at the Joint Staff J7 Human Geography Futures Seminar. Johns Hopkins Applied Physics Laboratory, June, 2014.

Wright A.L., (2013). Terrorism, Ideology and Target Selection. Department of Politics, Princeton University. Version 1.1. http://www.princeton.edu/politics/about/file-repository/public/Wright_on_Terrorism.pdf

Nontraditional Security Threats and a New Kind of Warfare

James M. Keagle[1]

The *global commons* has long been best understood as addressing tangible physical space that falls outside the governance of the state. The notion of parklands in urban areas and suburban communities has evolved from this tradition. The central challenge has always been collective responsibility and management of these lands—think water rights in the Western United States, equitable use was the dominant consideration. As the notion of global commons expanded beyond tangible land to management of its resources—such as fisheries or the world's ecosystem more generally—the requirement for responsible management shifted to supply management and protection of the planet's ecosystem. These spaces may also assumed increased geostrategic importance as strategic lines of communication. Now, the global commons in the 21st century security lexicon has expanded even further to consist of outer space and cyberspace. Together, the aforementioned constructs "*constitute the fabric or connective tissue of the international system,*" as Michèle Flournoy and Shawn Brimley noted in 2009.[2] This is not much different from the ideas geo-strategist Alfred Thayer Mahan expressed in *The Influence of Sea Power Upon History.* More than 100 years earlier he described the world's oceans as "*a great highway…a wide common.*"[3]

Today, as we push the envelope further regarding our understanding and the importance of the global commons, some suggest that the human species itself constitutes an essential element of the global commons and that human rights, equitable development, ethnic cleansing, and civil wars are legitimate parts of the expanding definition of the global commons. Regardless, the global commons is an important part of regional and global security and offers challenges and opportunities for cooperation as we share this planet.

Access to and development of the global commons remains important to an interconnected world. It is the notion that the use of the commons carries with it expense that brings with it fresh challenges. Part of this stems from the exploitation of the world's resources in the name of globalization and the growing realization that there are finite limits to the world's resources. Climate change add another dimension. Safe havens from which terrorists plan and launch their operations adds still another dimension. Finally, the emerging

[1] Keaglej@ndu.edu

[2] Flournoy M., Brimley S., The Contested Commons. *U.S. Naval Institute Proceedings.* July 2009: Vol. 135, No. 7. Note too that the inspiration for this work stems from the Global Commons Enterprise—a collaboration of NPS/CCMR. NDU/INSS, JFCOM/Joint Futures Group, and NATO/ACT. This introduction tracks closely with the July 2010 conference report introduction and specific charge, "Each partner may develop more detailed products related to the conference, as the conference was neither the start point, nor the end point for each member organization and their respective programs of research related to the issues in the global commons." The paper more broadly draws on previous follow-on work Keagle writings in 2012 (DTP 97).

[3] Mahan A.T., The Influence of Sea Power Upon History. In: Jablonsky D, ed. *Roots of Strategy: Book 4*. Mechanicsburg, PA: Stackpole Books; 1999: 3.

domains of space and cyber create new arenas for the states to contest—and develop conventions, rules and guidelines to regulate behavior. All of this suggests a world in which freedom of movement within the global commons may be increasingly competitive and constrained. Unlimited freedom to access and use the commons can and should no longer be taken for granted. Real and perceived scarcity must be addressed—not through conflict but rather through global and regional efforts to manage our planet and govern its inhabitants more responsibly.

Now, Russian president Vladimir Putin's claims of a resurgent *Novorossiya*, as well as the challenges posed by the Islamic State in Iraq and Syria (ISIS) in the borderless region of Syria/Iraq (refugees, displaced persons, and brutal terrorist tactics combined with effective military operations) threaten even more directly standard military operations and doctrine. The purpose of this article is to provide a better understanding of these security challenges and opportunities for expanded cooperation.

The Global Commons Under Siege

Three features of the current and expected operational landscape are most pressing, as noted in the 2010 U.S. *Quadrennial Defense Review*:

- Hybrid threats that blur traditional categories of conflict
- Assured access to and stability in the global commons
- Frequency and severity of problems with chronically fragile states.[4]

Each of these areas merits serious consideration and study.

The Hybrid Threat

What is a "hybrid" threat, and what makes it different from other kinds of threats? What should the United States expect regarding hybrid threats in the future? These threats are characterized by several features:

- Adversaries are likely to seize the initiative and employ a mix of conventional weapons, irregular tactics, weapons of mass destruction (WMD), terrorism, cyberattacks, and criminal behavior, supported by an information campaign.
- Higher and lower intensity forms of conflict often converge, blurring the categories and features of warfare.
- State or nonstate actors (or a combination thereof) employ a blend of two or more components of the spectrum of conflict, including economic, diplomatic, informational, and or/social domains.

The 21st century is filled with examples of these types of conflicts; two examples are the Hezbollah efforts in Lebanon in 2006 and the array of Arab Spring movements beginning

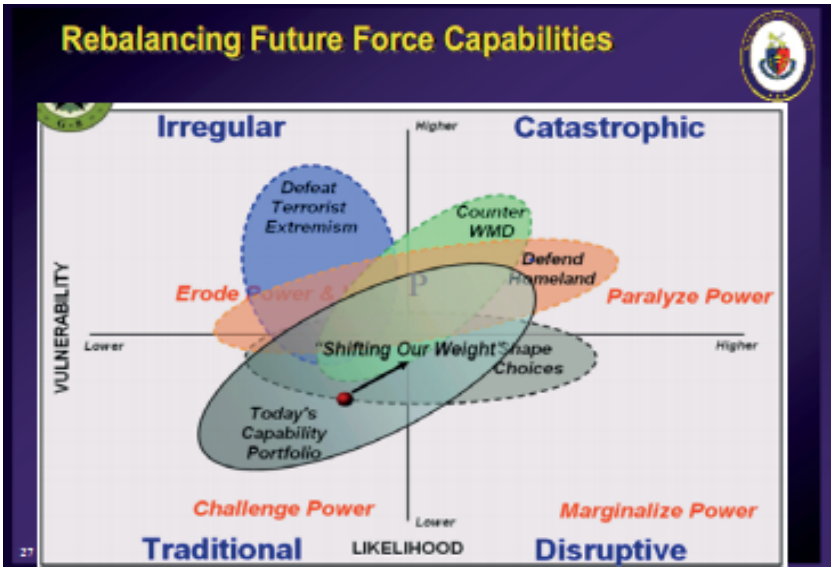
[4] Department of Defense. Quadrennial Defense Review. Title 10, U.S. Code, Subtitle A, Pt. I, Chapter 2, §118 (b) (1), February 2010. www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.pdf

in 2011 in the greater Middle East. Most recently, we have witnessed the Russian annexation of Crimea and further intervention in Ukraine in 2014 with a significant information warfare campaign.

The Islamic State of Iraq and Syria (ISIS) has launched brutal terrorist attacks on the peoples of Iraq and Syria under the pretense of establishing a caliphate. The movement's savage killings and information campaign to recruit support became a principal focus of the 2014 North Atlantic Treaty Organization (NATO) summit in Wales. This more complicated threat environment is captured in the next several illustrations.

The central message of Figure 1 is that force capabilities must adjust to meet new security challenges. As we shift up and to the right in the figure, the role of large conventional forces engaging one another diminishes and new requirements emerge. These new security challenges provide opportunities for collaboration and cooperation—as well as posing nontraditional threats to security establishments. This is likely to mean smaller conventional forces and greater attention to special operations forces, intelligence collection, and unmanned systems. More to the point, stability operations and irregular warfare have become co-equal with major military operations (traditional warfare). According to the 2008 Department of Defense (DOD) Directive 3000.07 on irregular warfare, "*It is Department of Defense policy to recognize that irregular warfare is as strategically important as traditional warfare. We must maintain capabilities and capacity to be as effective in irregular warfare as in traditional warfare. We must be capable of conducting irregular warfare independently of, or in combination with, traditional warfare.*"[5]

Figure 1. Shifting Our Weight

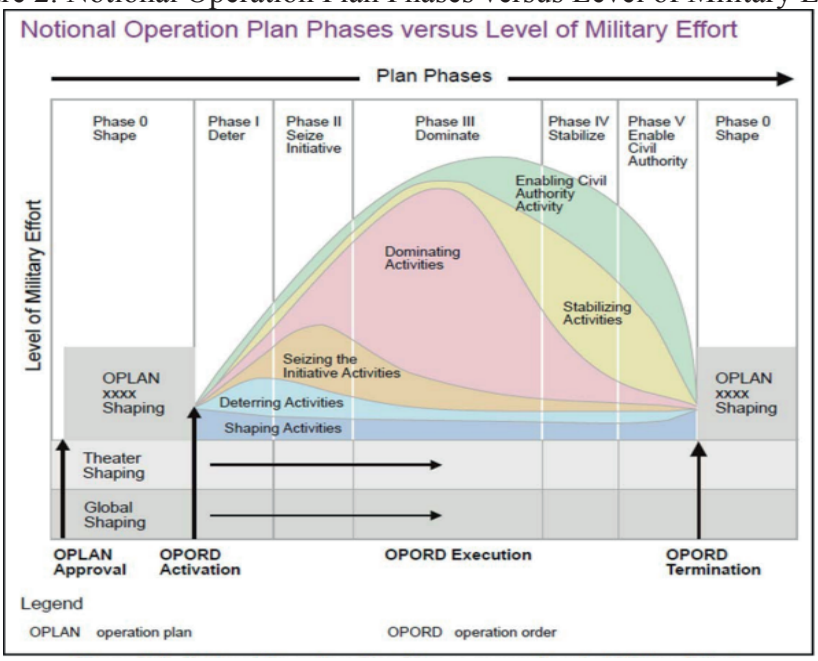


Source: 2006 U.S. Army posture statement, "21st Century Security environment: Our Era of Uncertainty and Unpredictability," available at www.army.mil/aps/06/04_21stCent.html

[5] Department of Defense Directive 3000.07. Irregular Warfare.l. December 1, 2008. http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/SWAAB/IW%20Reader/DoDD%203000.07%20IW%20Directive.pdf

Figure 2 even more dramatically tells the new story that avoiding war (Phase 0) is just as or more important than waging war or combat.[6] That means that even more resources and force structure will be diverted to the phases that precede and follow major combat operations (Phase III). Reinforcing this point, a recent the 2011 U.S. National Military Strategy states that stability and reconstruction missions (Phases IV and V) are now co-equal with major combat missions in terms of priority and importance.[7]

Figure 2. Notional Operation Plan Phases versus Level of Military Effort



Source: Joint Publication 3-0, *Joint Operations*, August 11, 2011.

Access to and Stability in the Global Commons

Perhaps the most pressing issue in the Asia-Pacific region is the People's Republic of China's (PRC) anti-access/area denial strategy. The PRC has leveraged military modernization programs combined with forward positioning of anti-ship ballistic missiles and economic and diplomatic policies into a position of greater influence. Arguably, by posing a greater threat not only to Taiwan but also to the U.S. Navy carrier battle groups, the PRC is causing other Asia-Pacific nations to reconsider their longer term political and military strategic alliances. The United States, for one, has announced the now oft-repeated pivot toward Asia—and taken steps to strengthen military and political ties with nations constituting the second island ring around China, much like its containment strategy against the Soviet Union during the Cold War. How all this plays out in the coming decades will largely shape the balance between conflict and cooperation in the region. Whether China is able to leverage the Shanghai Cooperation Council

[6] The White House. National Security Strategy of the United States. May 2010. www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

[7] Joint Chiefs of Staff. *The National Military Strategy of the United States of America.* Washington, DC: U.S. Department of Defense; 2011.

and other regional forums into effective tools of its long-term strategy of influence remains to be seen.[8]

The PRC has sought to wield this regional and global influence in the Arctic as well. The first step was to obtain observer status on the Artic Council in May 2013, followed quickly by announcing an expanded research and scientific polar institute. Climate change is beginning to open up the Northern Route as a potential revolution in the distribution of fossil fuel resources from supply locations to countries that are dependent on external sources for their energy needs. As the map in Figure 4 highlights, Russian territorial claims in the Arctic assert sovereignty over a strategically important potential fossil fuel transportation route. This becomes more than just a race to secure fossil fuel resources in the Arctic. The greatly reduced shipping distances via a route that hugs the Siberian coast (and may be under Russian control) may fundamentally diminish the value of the Malacca Straits and other key transportation networks that currently serve the world's commerce. The United Nations Convention on the Law of the Sea may prove insufficient to address these emerging issues.

Figure 4. Arctic Boundary Claims

Source: http://www.wired.com/images_blogs/wiredscience/2010/09/arctic-territory3.jpg

[8] Department of Defense Strategy for Operating in Cyberspace. July 2011. www.defense.gov/news/d20110714cyber.pdf

Incidents in similar contested spaces in the East China Sea (November/December 2013) and South China Sea (May 2014) suggest that longstanding conflicting claims to common spaces (with some economic or prestige value) remain at the forefront of interstate issues.

Chronically Fragile States

U.S. strategy has long concerned itself with economically and politically fragile states. Greater emphasis has been placed on this since the early days of the war on terror. Since 9/11, the language has included *ungovernable* or *ungoverned spaces*. A *governed space* is a geographic space over which a state authority has both the capacity and political will to exercise its sovereignty responsibly (for example, to maintain order and territorial integrity in conformity with the principles of secure international order based on state sovereignty). In an *ungoverned space*, state capacity and/or political will to exercise responsible sovereignty is absent. Ungoverned spaces can be further classified as *anarchic*, when a regime lacks the capacity to govern part or whole of country and no other actor has stepped in to fill the vacuum, and in the case of *competing governance*, when other actors attempt to fill the governance vacuum resulting from some mix of a regime's inability or unwillingness to govern subnational spaces or exercise specific governance functions. This concept does not address *ill-governed* spaces: regimes that use the principle of sovereignty as a shield behind which to engage in activities that pose threats to the international community.

By 2010-2013, our focus began to shift from Afghanistan-Pakistan to Yemen and al Qaeda in the Arabian Peninsula as an ungoverned space that provided a terrorist safe haven and the al Qaeda splinter group that operated with impunity therein. The geographic expansion continued into the Horn of Africa and the Maghreb—and by 2014 attention had turned to Iraq/Syria and ISIS. Within counterterrorism and counterinsurgency strategies, ungoverned spaces have become breeding grounds and sanctuaries for terrorist organizations to operate and conduct operations with impunity. What followed are capacity development programs to defeat, deter, and dismantle these organizations. Both in terms of governance capacity and political will, as Table 1 suggests, international cooperation will be key. Moreover, increased attention needs to be paid to recruitment locales, such as Karachi, versus sanctuaries.

Table 1. Capacity and Will

• Key components of governance capacity: o Security capacity (police, intelligence, paramilitary, military) o Administrative capacity (basic infrastructure, education system, public health and sanitation, public finance system) o Political capacity (channels for political participation, system of checks and balances, robust government organizations)
• Key components of political will: o Leaders' volition to exercise governance in conformity with the principles of a secure international order based on state sovereignty. Volition is shaped by cultural, historical and legal contexts o Leaders' willingness to expend resources and political capital to do so

Whether best understood as nation-building, stability and reconstruction operations, or long-term economic development, any development program will pose security challenges and opportunities for cooperation for the foreseeable future. One of these is the difficult challenge of discriminating between civil wars, wars of external aggression, and genocide. The world has taken a clear position on genocide: "never again." Yet obtaining consensus for collective action in these cases remain extremely difficult, however clear the facts on the ground may seem to some. As the world wrestles with a period of tight and austere budgets, finding the funds for long-term socio-political and economic development and war avoidance strategies will be difficult. The 2014 ISIS claims of a caliphate and military and recruiting success in the Syria/Iraq region directly challenge the West for an effective strategic response. Muslim/Arab and Western democracies must integrate their instruments of power into a coordinated effort to meet the threat. Topping the list of the tasks at hand are the following: addressing the government in Baghdad, ISIS savagery and genocide, ISIS economic pillaging of the oil and financial sectors, and its employment of social media recruitment methods.

While not limited to fragile states, humanitarian assistance and disaster relief (HADR) constitutes fertile ground for regional cooperation. Be it in response to the 2011 earthquake off the coast of Japan and subsequent tsunami and nuclear reactor breaches, or the tsunami that devastated Indonesia in 2008, HADR has been an essential element of the world's collective response to tragic natural events. The Transformative Innovation for Development and Emergency Support (TIDES) program shows initial promise for such collaboration. Its goals include leveraging global talent, integrating multiple approaches, and sustaining longer term development through private sector investment. It supports the basic needs of stressed populations by focusing on key infrastructures—water, power, shelter, cooking, cooling and heating, lighting, sanitation, and information and communications technology. TIDES goes beyond HADR to broader support for civil authorities and building their general capacities.[9]

[9] See the STAR-TIDES Web site at www.star-tides.net for a more complete description of the TIDES program.

The Challenge of the Global Commons

Whether understood as air, land, sea, cyber, or space, these domains of the global commons comprise the infrastructure on which the global system operates and through which its major components—information, people, commerce, finance, technology, or military muscle—flow. Individual, national, and global prosperity and governance depend on this interconnected and interdependent network of relationships that operate within and across these domains. Prosperity and freedom can be enhanced or threatened depending on how security challenges and regional cooperation efforts are balanced.

Outer Space

Society has become dependent on capabilities and information delivered to, from, and through space. Perhaps the most dramatic of these examples is the prosecution of the war against al Qaeda. While some of the operational details remain unknown to the general public, it is commonly understood that the combination of special operations forces and intelligence officers relies on outer space to transmit data in near real time regarding the location of individual human targets and the subsequent application of lethal force (via drones) across international airspace and sovereign borders. This new kind of warfare may define conflict for the next several decades.

Furthermore, resourceful adversaries may leverage asymmetric technologies and unconventional approaches to circumvent traditional advantages, negate core strengths, and exploit vulnerabilities of competing forces. They could exploit the outer space commons in a variety of challenging ways:

- Offensive computer network operations and electronic warfare with kinetic first strikes could disrupt battlefield network information and space systems.
- Space systems could deny the use of reconnaissance, early warning, communications, navigation, and weather satellite assets that enhance land-based military operations.

Equally important, we have become highly dependent on space for more routine communications, be it the use of global positioning systems for everyday transport of goods, people, and services from one location to another, or the more secure transmission of information that is the lifeblood of international financial markets. Figuring out the rules and codes of conduct that should govern this domain is both a commercial and governmental responsibility—and one that demands cooperation and reconciliation of competing views and cultures. It goes far beyond simple declarations regarding prohibitions on weapons in space or antisatellite weapons. Space debris poses dangers in space, and when it falls to Earth, may threaten people in its path. Space law and emerging capabilities regarding co-orbital intercept systems, attribution, proportionality, and escalation (breaking through previously declared red lines) all merit significant international attention. Lastly, no one in the Asia-Pacific theater can ignore the challenges that WMDs pose. Cooperative ballistic missile defense offers one area of cooperation for peacefully managing the global commons and addressing those who pursue provocative military policies.

Airspace

Closely related to the challenges WMDs pose in space, ballistic missiles and cruise missiles could threaten ships at sea, civilian population centers, or military build-up areas. Fourth-generation fighter aircraft and sophisticated air defense weapons could put in question local air supremacy or superiority.

Drones and other remotely operated or unmanned systems provide challenging international issues as we target terrorists hiding in sanctuaries. We face an immediate future in which domestic airspace will be a focus of the debate about the use of drones. We need to wrestle with the legal and airspace management issues associated with these systems operating over the homeland—and the pass-off challenges as the systems cross international boundaries.

Maritime

While state actors have been the traditional threat in regard to interrupting or denying lines of communications and challenging assured access to strategic resources, nontraditional threats are reemerging and are worthy of regional efforts to diminish if not deny their effect. Maritime terrorists, pirates, and criminal organizations are appearing with increasing frequency and complicate the defense challenges in the maritime domain. Swarming as an operational tactic has become increasingly common, and will likely continue to be so. Since the "enemy" often enjoys the advantages of seizing the initiative in battle, our forces must also adopt similar attributes of flexibility and speed (and stealth) to be able to respond in time. This will undoubtedly require cooperation and collaboration in information and intelligence sharing as well as potentially pooling national assets.

Expanded interests in off-shore resource development and exploitation also offer opportunity for cooperation as well as conflict. Be it energy in the Spratly Islands or the Arctic or minerals ripe for deep seabed mining, we will need more cooperation in the future to address the challenges of prosperity, peace, limited resource supply, and growing resource demand.

Land

Perhaps the two most dramatic examples of this changing domain come from Central and South Asia. First, the International Security Assistance Force operation felt the pain of its curtailed land route through Pakistan using Karachi as a port of entry. The Northern Transportation Network, which is much more dependent on air bridges, ultimately proved satisfactory—but at a much higher cost.

Second, as the international community seeks opportunities for the economic development of Afghanistan, it is constantly reminded of the challenges of landlocked states. The future is often linked to a modern-day Silk Road, with trucks replacing camels and pack mules as the preferred mode of transportation. Moreover, if Afghanistan can finds ways to unlock its projected mineral wealth, then more will flow on these new roads than silk rugs and tea. Still, the inherent

advantages of maritime transportation make forecasting the economic success of a new Silk Road problematic.

Cyberspace

U.S. policy spokespersons repeatedly identify cyber as the greatest single security threat. Cyberspace integration brings new levels of vulnerability and the potential for mass disruption of infrastructures or functions across critical military, political, and economic targets. Complicating the challenge is that the overwhelming majority of targets are in the private sector, demanding a degree of cooperation and (classified and sensitive) information sharing across boundaries rarely crossed in the past.

The DOD Cyber Strategy was released in 2011. It is intended for the whole of government and contains five strategic initiatives:

1. Treat cyberspace as an operational domain to organize, train, and equip so that DOD can take full advantage of cyberspace's potential.
2. Employ new defense operating concepts to protect DOD networks and systems.
3. Partner with other U.S. Government departments and agencies and the private sector to enable a whole-of-government cybersecurity strategy.
4. Build robust relationships with U.S. allies and international partners to strengthen collective cybersecurity.
5. Leverage the Nation's ingenuity through an exceptional cyber workforce and rapid technological innovation.[10]

Strategic initiative 4 addresses directly the need for international cooperation:

> "*The development of international shared situational awareness and warning capabilities will enable collective self-defense and collective deterrence. By sharing timely indicators about cyber events, threat signatures of malicious code, and information about emerging actors and threats, allies and international partners can increase collective cyber defense. Cyberspace is a network of networks that includes thousands of ISPs [Internet service providers] across the globe; no single state or organization can maintain effective cyber defenses on its own.*"[11]

At least two specific concerns complicate the problem for international and national security specialists:

- Advanced persistent threat–class malware attacks (targeted, zero-day, stealthy) are real world possibilities.
- While cyberspace relies on the digital infrastructure of individual countries, such infrastructure is globally connected.

[10] Department of Defense Strategy for Operating in Cyberspace. July 2011. www.defense.gov/news/d20110714cyber.pdf
[11] Ibid.

We are faced with similar challenges to those discussed already regarding space: domain incident characterization, attribution determination, firewalls versus active defense mechanisms in an asymmetric environment, proportionate retaliation, and the enforcement and adjudication mechanisms. An international cooperation regime seeking to support responsible behavior and oppose and dissuade those who seek to disrupt network systems would need to share warning capabilities, engage in capacity building, and conduct joint training activities.[12]

Since criminal exploits, military or industrial espionage, critical infrastructure infiltration or sabotage, and nationalist hacker protests might represent elements or techniques of cyberwarfare, figuring out appropriate cooperative as opposed to individual responses will be difficult. Such increased sharing and cooperation is far simpler to describe in a strategy document than to implement in practice. Some of the tough questions that demand common answers follow.

Incident Characterization in Cyberspace

- Is cyber warfare characterized as simply "*an armed conflict conducted in whole or part by cyber means?*" (JCS Joint Terminology)
- In addition to "*military operations to deny an opposing force the effective use of cyberspace systems and weapons,*" how does the world commonly address cyber intrusions on governmental services, financial enterprises, and media outlets? Would attacks cross the threshold for an act of war if adversaries cause physical damage to energy, water, or transportation systems?

Attribution Determination in Cyberspace

The difficulty in identifying attackers with a high degree of confidence in a timely manner complicates deterrence, preemption, and common response strategies. Botnets and proxy servers enable attackers to operate with anonymity and impunity. Advanced persistent threats conceal or avoid detection of attacker identities. Challenges in detecting attacks or breaches and attributing correctly delay target identification and retaliatory response. Failure to detect intentions, moves, and origins stalls preemption and could lead to overreactions and miscalculations.

One solution to the threat of cyberattacks is resilient, layered, active cyber defenses. However, ownership of these defenses and the proper burden sharing responsibilities are unanswered questions that still need to be addressed. Is this a shared responsibility? What is the nature of the (financial) burden sharing? Protecting the computers, networks, and control systems in defense and civilian sectors requires a multilayered, defense-in-depth strategy that wields active security defenses. What does active defense mean? Sniping?

One place to begin is with protecting civilian and military cyberspace physical assets (computers, servers, controllers, cables, transmitters, satellites, and sensors—the potential targets) and their vulnerabilities. Next, national and collective responses are needed to develop capabilities, including protocol filters, content sensors, behavioral anomaly scanners, and forensic analysis, to

[12] The White House. National Security Space Strategy. January 2011. http://www.defense.gov/home/features/2011/0111_nsss/.

detect and stop, or discover and mitigate, malicious activity. Again, we need a significant investment in resources for these detection capabilities and a common agreement as to what constitutes malicious activity.

Obviously, this demands public, private, and international partnerships that share threat intelligence, analyze vulnerabilities, and identify risk mitigation strategies. This is far easier to describe in words than execute in practice, particularly in an environment that long operated on a need-to-know basis and with very limited sharing across national and bureaucratic boundaries.

Proportionate Retaliation in Cyberspace—and the Cross-Domain Challenge

Even if the attackers are known with certainty, a challenge exists in determining which incidents justify responses that involve specific uses of force.

- What are the thresholds? Substantial deaths, secondary kinetic damage, or cascading economic losses could justify proportionate retaliation by cyber or kinetic means.
- Does a right to counterstrike in self-defense exist if attackers target financial systems, public sectors or utilities such as power grids, communications networks, or critical defense industries?
- If origins are traced and force is the response, can collateral damage be avoided or limited to acceptable levels if the intrusions were launched through thousands of hijacked computers in third-country or target nation sites?
- Key role of signaling—how will the various actors in the "partnership" interpret the event and construct a common response that clearly and unambiguously signals intent and intended consequences (in order to avoid an escalation spiral)?

Overlapping Jurisdictions

Transnational cyber incidents underscore overlapping jurisdictions that pose control concerns for prosecution.

- If an attack originates from servers linked to multiple sources, sufficient evidence might not exist to confirm an endorsed attack from a single or multiple sources/governments; if the source is not a nation, what is the response, and against whom is it targeted?
- Some transnational investigative cooperation is required to enforce a commonly agreed body of criminal laws and to prosecute actors for attacks generated from sovereign territory, and it is complicated by routing of attack traffic and information acquired through compromised servers in a third-party country. What will be the venue for developing that internationally accepted body of law? How will differing standards of privacy be reconciled?
- Some countries may not be willing to compromise sources and methods to reveal knowledge.
- Some countries may not be willing to acknowledge they are blind to a specific event and need outside assistance (acknowledging a vulnerability).

- The best and most timely information may be in hands of the private sector (much like CNN effect that competed with our intelligence community for the ear of the commander in the 1980s); there is a growing body of research about crowd sourcing in the era of social networks that needs common attention.[13]
- Prosecution of enraged citizens, dedicated activists, and criminal elements, many of whom reside outside the targeted nation, might not still be feasible given attribution challenges and legal costs. All of this returns to the discussion of failed or near-failed states and their vulnerabilities.

One obvious conclusion is that internationally acceptable rules could promote order in cyberspace by encouraging states to meet their duties in protecting citizens from crime, upholding the right of self-defense, and applying rules of modern warfare. But that will be a long and difficult road to navigate.

Role of Defense Capabilities in Cyberspace

Defense capability development considers how to counter competitors who wage warfare in the commons. The identification and fielding of overwhelming force, both as a deterrent and a defensive capability, might include abilities in the following areas:

- the traditional use of firewalls for data and critical infrastructure protection
- vulnerability mapping and anomaly detection
- attack mitigation and resiliency
- active defenses

It is worth noting that General James Cartwright, USMC (Ret.), former Vice Chairman of the Joint Chiefs of Staff, noted in May 2012 that the United States needed to protect its military systems, including the stealthy F-35 Joint Strike Fighter, from hackers: "*That's the reality of the battlefield we are going to be in.*" Cartwright went on to add that "*in military terms of offense and defense we are thinking 90 percent defense, 10 percent offense. That is 'bass-ackwards' for us. Our job is to kill things.*"[14] This theme was reinforced with the public release of the Defense Advanced Research Projects Agency's efforts on Plan X. As Ellen Nakashima reports, this is part of an "*ambitious effort to develop technologies to improve cyberwarfare capabilities, launch effective attacks and withstand the likely retaliation.*" Or, as she summarizes, this "*push marks a new offensive phase.*"[15]

One way to move ahead in this new world is to emulate NATO's Smart Defense concept among partners worldwide. According to Henrik Breitenbauch and Bastian Giegerich, Smart Defense is a game-changer regarding defense planning and weapons procurement, in that it is based on true

[13] Department of Defense Strategy for Operating in Cyberspace, 9.
[14] Pincus W., Retired General Talks Frankly on Defense. *The Washington Post*. May 22, 2012: 9A. http://www.washingtonpost.com/world/national-security/retired-gen-james-cartwright-offers-a-fresh-view-on-defense/2012/05/21/gIQArRMTgU_story.html
[15] Nakashima E., U.S. Builds a Cyber 'Plan X'. *The Washington Post*. May 31, 2012; A1, A6. http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

international cooperation. They conclude that international burden sharing is a must—and that products and projects must "*include partners from two or more allied nations.*"[16] Some areas for possible collaboration are noted below.

Space Assurance, Sea Control and Air Superiority

As rivals look for opportunities to degrade U.S. control over the global commons, they will increasingly look to asymmetric avenues to attack U.S. interests. Areas of the global commons where the U.S. is virtually unchallenged—specifically space, sea, and air—will be threatened by states and non-state actors using elements of hybrid warfare.

While weapons systems designed to strike satellites are probably out of reach for most non-state actors, states will continue to look to ways to gain an advantage in space. In 2007, the PRC shot down a defunct Chinese satellite using a ground based missile system. Since then, the PRC has continued to develop their ability to strike space based assets. There are several ways that the U.S. can respond. Improved satellite protection, including redundancy, data encryption, physical hardening, and increased maneuverability will be critical. Emphasis on space situational awareness must improve in order to help the U.S. determine the intentions and attributing actions of foreign actors regarding U.S. space assets. Finally, U.S. space based systems must have a rapid reconstruction capability in order to replace critical assets that have been destroyed or disabled.[17] Recent initiatives from OSD Space Policy have begun to develop a common vocabulary for space resilience. Be they in the form of disaggregated, diversified, proliferated, or distributed systems that rely on active and passive countermeasures and deception, such efforts must be in balance with deterrent initiatives to maximize the survivability and recovery of space assets.

Opponents will attempt to counter overwhelming U.S. sea and air power in the same fashion. Instead of direct challenges, rivals will develop capabilities to destroy or disable U.S. naval and air assets through irregular avenues. The U.S. should respond by hardening fleet protection and seeking to destroy enemy combat networks that enable their hybrid capabilities. Degradation or destruction of enemy air defense systems will be crucial in order to allow U.S. air power to operate in hostile situations. The Observe, Orient, Decide, Act loop (OODA Loop) needs to evolve to account for compressed time horizons. The need to "shoot first" will lead us towards rules of engagement and predetermined firing procedures will take humans further from the decision loop to employ lethal force in specific situations.

A New Kind of Warfare

Beyond the global commons is a contest for the loyalty of and political dominion over ethnic nationalities around the globe. Putin calls this *Novorossiya*. He has laid claim to Crimea and pressured other neighboring countries (Latvia, Estonia, Moldova, Kazakhstan) with large

[16] Breitenbauch H., Giegerich B., A Smart Opportunity. *Defense News*, May 21, 2012. http://archive.defensenews.com/article/20120520/DEFFEAT05/305200007/A-8216-Smart-8217-Opportunity.
[17] Shalal A., Analysis points to China's work on new anti-satellite weapon. *Reuters*. March 17, 2014. http://www.reuters.com/article/2014/03/17/us-china-space-report-idUSBREA2G1Q320140317

Russian minorities. Thugs, criminal gangs, and volunteers better describe the adversary—not soldiers.

Military intelligence and special operations forces permeate the leadership of such groups that operate with or without uniforms. They tend to rely on light weapons rather than tanks, planes, and ships. Operations tend to include systemized and organized attacks on police stations, government buildings, and the like, not attacks on large or small military units. They pursue flexible goals based on the resistance encountered, with no fixed timetables for victory. Almost always, this new kind of warfare includes a heavy dose of propaganda targeted at ethnic groups—the idea of "*coming home to Mother Russia,*" for example. This poses both political and military new challenges for militaries. Avoiding civil wars and confronting the adversary directly will be increasingly difficult in this new security environment.

Implications for Future Military Operations

These changes will shape tomorrow's Joint Forces. The traditional size and composition emphasis on large forces with heavy firepower will be increasingly vulnerable and ineffective in the new security environment. More agile and flexible forces that can operate in austere environments with limited infrastructures will more likely define the future force. Resources will need to be shifted from carrier battle groups, air supremacy fighter wings, and armor and artillery units to special forces, intelligence operatives, and drones. The Joint Force will need to increase its resourcing of the cyber and space domains as well as culture and language education and training. The Joint Force will also need to develop specialists in communications attuned to messaging and counter-narratives.

Conclusions

Nontraditional security threats increasingly occupy the time and resources of national security professionals. The cyber domain has the attention of many of us, but other domains also are rife with threats and opportunities for collaboration and cooperation. Given the broad array of threats across a number of domains, the Asia-Pacific region should expand its emphasis on cooperative efforts to reduce the likelihood of war—and if that fails, mitigate its effects. These new threats pose enormous challenges in developing a common value base. Following through with a shared set of responses will require constant vigilance and perhaps nearly instantaneous or even pre-emptive actions in order to protect and advance the security, prosperity, and freedom of like-minded nations and peoples. Ultimately, protecting these interests may require the supreme sacrifice of blood and treasure. We must hope that we are up to the challenge.

References

Breitenbauch H., Giegerich B., A Smart Opportunity. *Defense News,* May 21, 2012. http://archive.defensenews.com/article/20120520/DEFFEAT05/305200007/A-8216-Smart-8217-Opportunity.

Department of Defense. (2010). *Quadrennial Defense Review.* Title 10, U.S. Code, Subtitle A, Pt. I, Chapter 2, §118 (b) (1). www.defense.gov/qdr/qdr%20as%20of%2029jan10%201600.pdf.

Department of Defense Directive 3000.07. *Irregular Warfare l.* (2008) http://www.mccdc.marines.mil/Portals/172/Docs/SWCIWID/SWAAB/IW%20Reader/DoDD%203000.07%20IW%20Directive.pdf.

Department of Defense Strategy for Operating in Cyberspace. (2011). www.defense.gov/news/d20110714cyber.pdf.

Flournoy M., and Brimley S., (2009). The Contested Commons. *U.S. Naval Institute Proceedings. Vol. 135,* No. 7.

Joint Chiefs of Staff. (2011). *The National Military Strategy of the United States of America.* Washington, DC: U.S. Department of Defense.

Mahan A.T., (1999) The Influence of Sea Power Upon History. In: Jablonsky D, ed. *Roots of Strategy*: Book 4. Mechanicsburg, PA: Stackpole Books. 3.

Nakashima E., (2012). U.S. Builds a Cyber 'Plan X'. *The Washington Post.* May 31. A1, A6. http://www.washingtonpost.com/world/national-security/with-plan-x-pentagon-seeks-to-spread-us-military-might-to-cyberspace/2012/05/30/gJQAEca71U_story.html

Pincus W., (2012). Retired General Talks Frankly on Defense. *The Washington Post.* 9A. http://www.washingtonpost.com/world/national-security/retired-gen-james-cartwright-offers-a-fresh-view-on-defense/2012/05/21/gIQArRMTgU_story.html

Shalal A., (2014). Analysis points to China's work on new anti-satellite weapon. Reuters. http://www.reuters.com/article/2014/03/17/us-china-space-report-idUSBREA2G1Q320140317.

The White House. (2010). *National Security Strategy of the United States.* www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

The White House. (2011). *National Security Space Strategy.* http://www.defense.gov/home/features/2011/0111_nsss/.

The Future Evolution of Transnational Criminal Organizations and the Threat to U.S. National Security

Celina B. Realuyo[1]

Combating transnational criminal and trafficking networks requires a multidimensional strategy that safeguards citizens, breaks the financial strength of criminal and terrorist networks, disrupts illicit trafficking networks, defeats transnational criminal organizations, fights government corruption, strengthens the rule of law, bolsters judicial systems, and improves transparency. While these are major challenges, the United States will be able to devise and execute a collective strategy with other nations facing the same threats.

— U.S. National Security Strategy, May 2011[2]

Overview

In the 21st-century global security environment, we are facing a complex set of threats to U.S. national security emanating from state and non-state actors. These threats endanger the key responsibilities of the nation-state to its citizens: to guarantee their security and the nation's territory, promote economic prosperity, safeguard society, and ensure that the government represents their will. Illicit networks that include terrorists, criminals, and proliferators are presenting unprecedented asymmetrical threats to U.S. interests at home and abroad. The tragic September 11, 2001, attacks perpetrated by al Qaeda are just one such example of threats from non-state actors.

Besides terror groups, transnational criminal organizations (TCOs) are among the non-state actors that leverage their illicit activities, immense resources, and use of violence to undermine the security and prosperity of the United States and partner nations. The United States recognizes TCOs as a national security threat and has deployed a national security strategy to combat it. In order to attack these networks, the United States must understand and deny access to critical enablers needed by TCOs to operate.

The future trajectory of transnational criminal organizations is disconcerting, as they will seek to penetrate new markets with goods and services and establish more spheres of influence using corruption and violence. The cyber domain will afford them a new operating environment to further expand their criminal activities. Some TCOs will continue to resemble multinational corporations focused on maximizing profits, while others will hijack political power in the form of criminalized states. Another dangerous and disturbing evolution that we are already witnessing is the convergence of terrorism and crime where groups use criminal proceeds to fund terrorist activities. To combat the evolution of these threats, the Joint Force will need to develop more innovative kinetic and non-kinetic measures and build its own networks to neutralize transnational criminal networks.

---

[1] RealuyoC@gc.ndu.edu

[2] The White House. National Security Strategy of the United States. May 2010; www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

The Transnational Criminal Organization Threat to U.S. National Security

Globalization has dramatically improved our quality of life over the past 30 years, providing us with products, services, information, and technology—faster, cheaper, and better. We have seen, however, a darker side of globalization, with terrorism, armed conflict, international crime, movement of U.S. jobs to overseas markets, and economic crises dominating our headline news. Non-state actors, including criminals, terrorists, and proliferators, leverage the global marketplace with illicit activities to promote their respective interests around the world; such activities threaten the national security of the United States and its allies. The transnational trafficking of drugs, arms, people, and counterfeit goods and the money laundering that accompanies these illicit activities compromise the safety of consumers, rob inventors of their intellectual property, deny governments significant tax revenues, and undermine our economies. In contrast to nation-states or terrorist groups with political or ideological aspirations, transnational criminal organizations (TCOs) are driven primarily by *greed*. According to the White House definition, *transnational organized crime* (TOC) refers to:

> *those self-perpetuating associations of individuals who operate transnationally for the purpose of obtaining power, influence, monetary, and/or commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and/or violence, or while protecting their illegal activities through a transnational organizational structure and the exploitation of transnational commerce or communication mechanisms.*[3]

Crime and corruption have existed since the dawn of civilization and traditionally have been addressed as local security issues. In an age of globalization, the scale and velocity of transnational organized crime, driven by interconnected economies and technological advances and engendering record levels of violence, have transformed it into a global security threat. According to Admiral James Stavridis, USN (Ret.):

> *Criminal networks have the advantage of three primary enablers. First are the huge profits realized by transnational criminal operations. Second is the ability of these organizations to recruit talent and reorganize along lines historically limited to corporations and militaries. The third is their newly developed ability to operate in milieus normally considered the preserve of the state, and often referred to as the diplomatic, informational, military, and economic elements of national power.*[4]

TCOs do not respect the rule of law, sovereignty, or human rights, and they wield impressive resources to promote and realize their illicit activities.

In many cases, international drug cartels, mafias, and gangs are better armed, funded, and trained than the government security forces charged with confronting them. TCOs exploit ungoverned

[3] National Security Council. Strategy to Combat Transnational Organized Crime: Definition. www.whitehouse.gov/administration/eop/nsc/transnational-crime/definition.

[4] Stavridis J., Foreword. In: Miklaucic M., Brewer J., eds. *Convergence: Illicit Networks and National Security in the Age of Globalization.* Washington, DC: NDU Press; 2013.

spaces and fragile states to conduct their operations and even hijack the nation-state. More disturbing has been a dangerous convergence of terrorism and crime that is becoming a formidable threat to nation-states. Such is the case with the Haqqani network in Afghanistan, the FARC in Colombia, al Qaeda in the Islamic Maghreb, and Hezbollah's global networks leveraging illicit activities to realize their terrorist agendas.[5] As globalization and technological innovation proceed in the future, transnational criminal organizations will continue to capitalize on the drivers of globalization and evolve as a critical transnational threat to our national security and that of our allies.

U.S. Strategy to Combat Transnational Organized Crime

In July 2011, the White House released the U.S. Strategy to Combat Transnational Organized Crime (CTOC) that clearly identifies TCOs as a national security threat to U.S. prosperity and security through their various illicit activities. The strategy calls for multilateral action to constrain the reach and influence of TCOs, deprive them of enabling means and infrastructure, shrink the threat they pose to citizen safety, national security, and governance, and ultimately defeat the TOC networks that pose the greatest threat to national security. The Mexican Sinaloa Cartel, Lebanese Hezbollah, Moscow Center/Brothers' Circle, and Dawood Ibrahim's "D Company" in India are among the most dangerous TCOs challenging state sovereignty and national security around the world.

The U.S. CTOC strategy is organized around a single unifying principle: to build, balance, and integrate the tools of American power to combat transnational organized crime and related threats to national security—and to urge our foreign partners to do the same. The endstate we seek is to reduce transnational organized crime from a national security threat to a manageable public safety problem in the United States and in strategic regions around the world. The strategy will achieve this end state by pursuing five key policy objectives:

- Protect Americans and our partners from the harm, violence, and exploitation of transnational criminal networks.
- Help partner countries strengthen governance and transparency, break the corruptive power of transnational criminal networks, and sever state-crime alliances.
- Break the economic power of transnational criminal networks and protect strategic markets and the U.S. financial system from TOC penetration and abuse.
- Defeat transnational criminal networks that pose the greatest threat to national security by targeting their infrastructures, depriving them of their enabling means, and preventing the criminal facilitation of terrorist activities.
- Build international consensus, multilateral cooperation, and public-private partnerships to defeat transnational organized crime.

The strategy also introduces new and innovative tools and capabilities that will be accomplished by prioritizing the resources available to affected departments and agencies. This includes taking

[5] Realuyo C.B., Hezbollah's Global Facilitators in Latin America. *Terrorist Groups in Latin America: The Changing Landscape*: testimony before the Subcommittee on Terrorism, Non-Proliferation, and Trade, House Committee on Foreign Affairs, U.S. House of Representatives. February 4, 2014. http://docs.house.gov/meetings/FA/FA18/20140204/101702/HHRG-113-FA18-Wstate-RealuyoC-20140204.pdf.

the following measures:

- A new executive order will establish a sanctions program to block the property of and prohibit transactions with significant transnational criminal networks that threaten national security, foreign policy, or economic interests.
- A proposed legislative package will enhance the authorities available to investigate, interdict, and prosecute the activities of top transnational criminal networks.
- A new Presidential proclamation under the Immigration and Nationality Act will deny entry to transnational criminal aliens and others who have been targeted for financial sanctions.
- A new rewards program will replicate the success of narcotics rewards programs in obtaining information that leads to the arrest and conviction of the leaders of transnational criminal organizations that pose the greatest threats to national security.
- An interagency Threat Mitigation Working Group will identify those TOC networks that present a sufficiently high national security risk and will ensure the coordination of all elements of national power to combat them.[6]

Critical Enablers of Transnational Criminal Organizations

To combat transnational criminal organizations, we must understand their motivations, operations, strengths, and vulnerabilities. Driven by greed, they resemble business enterprises in the legitimate private sector, seeking to match supply and demand in the market. Just like other organizations, TCOs require the following critical enablers to sustain their activities and realize their objectives (see figure 1):

- *Leadership*. TCOs require leadership that marshals, directs, and manages resources to achieve their mission of maximizing profits. TCO leadership can be organized as hierarchies or, more likely, as loose networks of affiliates that diversify the "key man risk" associated with relying on a sole leader for command and control.

- *Illicit activities*. TCOs engage in a broad spectrum of illicit revenue-generating activities including trafficking in narcotics, arms, humans, exotic wildlife, and contraband, as well as money laundering, cybercrime, extortion, and kidnapping for ransom.

- *Logistics and supply chains*. TCOs rely on global supply chains, commercial transportation, TCO-owned resources, and other logistical support to move materiel, personnel, services, and funding from supply to demand points of their enterprises.

- *Personnel*. TCOs must recruit and maintain personnel to support all aspects of their activities.

- *Financing*. TCOs consider revenue as both a key objective and an enabler. Financing serves as the lifeblood for TCOs and their illicit endeavors; they derive power from their

[6] National Security Council. Strategy to Combat Transnational Organized Crime: Executive Summary. www.whitehouse.gov/administration/eop/nsc/transnational-crime/summary.

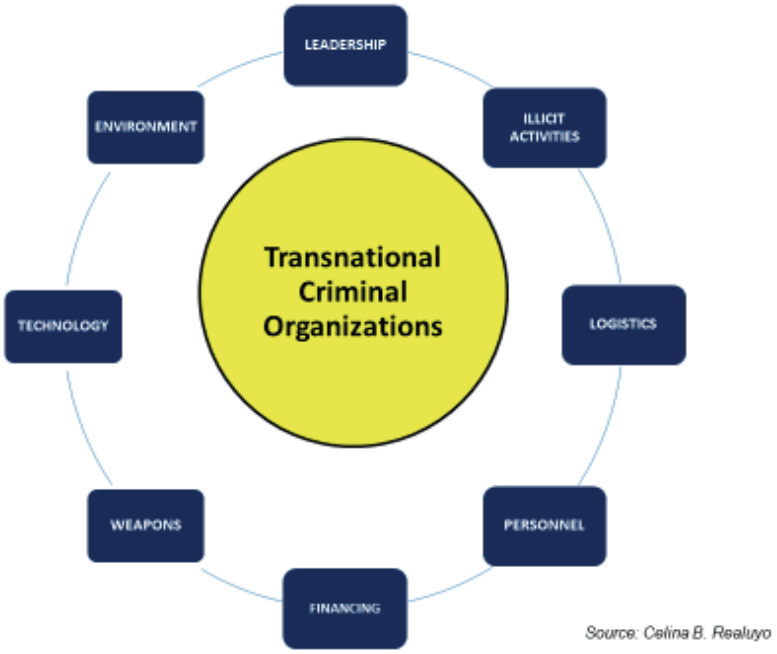
wealth and use it to corrupt and co-opt rivals, facilitators, and/or government and security officials.

- *Weapons*. TCOs use force or the threat of force to dominate their operating areas; therefore, access to weapons, the ability to deploy them, and their lack of concern for collateral damage make TCOs so violent and lethal.

- *Technology and communications*. TCOs assiduously adopt new technology and communications methods to avoid detection by security forces and monitor and adapt to changes in their areas of operation.

- *Operating environment/corruption*. TCOs enjoy operating in ungoverned or weakly governed spaces where state control and oversight are lacking or can be compromised. While they may not necessarily aspire to topple and replace governments, they seek out officials vulnerable to corruption who can facilitate TCO activities in certain geographic areas.[7]

Figure 1. Critical Enablers of Transnational Criminal Organizations



Washington and other national governments must understand the critical enablers, vulnerabilities, and motivations of TCOs to better detect, disrupt, dismantle, and deter them from undermining our security and prosperity. The United States can effectively combat TCOs by limiting, denying, or neutralizing their access to these critical enablers and resources. Toward this end, every instrument of national power (diplomatic, military, intelligence, law enforcement,

[7] Realuyo C.B., Collaborating to Combat the Convergence of Illicit Networks. Lecture delivered at Harvard University, John F. Kennedy School of Government, South Asian Senior National Security Seminar. May 1, 2014. Cambridge, MA.

information, financial, and economic) must be leveraged to effectively implement the 2011 Strategy to Combat Transnational Organized Crime.

The Future Evolution of Transnational Criminal Organizations

Transnational criminal organizations are highly adaptable, constantly responding to supply and demand factors, their operating environment, and government countermeasures. Since TCOs are market-driven, they will seek out new sources and markets for their goods, services, and operations. As emerging markets become more affluent, TCOs will continue to expand their illicit activities around the world. A new frontier, the cyber domain, will further empower TCOs as they capitalize on new opportunities for illicit activities in cyberspace and incorporate new technologies to further improve their operations. According to INTERPOL, cybercrime is outpacing other forms of criminal activities with incalculable profits. More and more criminals are exploiting the speed, convenience, and anonymity of the Internet to commit a diverse range of criminal activities that knows no borders, either physical or virtual.[8] While many TCOs will operate like large multinational corporations, in some cases they will act more like nation-states as they expand control over their operating spaces, resources, and populations and directly threaten U.S. interests at home and abroad.

TCOs will continue to organize as networks of affiliates and perhaps specialize in distinct illicit activities like cybercrime, human trafficking, or money laundering. For example, the ruthless Mexican cartel Los Zetas is concentrating on human trafficking and extortion rather than narcotics trafficking, which is dominated by their powerful rival, the Sinaloa Cartel. They posit that alien smuggling and human trafficking are extremely profitable, deriving income from a renewable resource (people); in addition, this form of crime incurs lower risks and penalties than drug trafficking.[9] This case illustrates how quickly TCOs respond to economic drivers and government countermeasures to transform their illicit enterprises. The networked and flat nature of TCOs complicates the use of classic attacks on organizational leadership and command and control structures against them; comprehensive new approaches will be required to degrade them.

The Criminalized State

To secure their freedom of movement, operating space, and supply chains, TCOs will seek to corrupt, co-opt, infiltrate, and even take over state institutions. A few years ago, analysts were predicting state failure in Mexico, as the Mexican cartels were becoming more violent and powerful in the face of an aggressive military offensive against them under former President Felipe Calderon. Human Rights Watch estimates that over 60,000 were killed in the Mexican drug war from 2006 to 2012.[10] Despite these record levels of violence, the Mexican cartels did not seek to overthrow and replace the central government. However, they were intent on

[8] INTERPOL. Cybercrime. www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[9] Texas Department of Public Safety (2014). *Assessing the Threat of Human Trafficking in Texas*. www.dps.texas.gov/director_staff/media_and_communications/2014/txHumanTraffickingAssessment.pdf.
[10] CNN. Mexico's Drug War: Fast Facts. http://www.cnn.com/2013/09/02/world/americas/mexico-drug-war-fast-facts/.

safeguarding their trafficking routes and operating areas; security analysts actually attribute many of the deaths to inter- and intra-cartel violence to dominate or eliminate each other.[11] This lack of interest in political regime change by the Mexican cartels may not be the model all TCOs ascribe to in the future.

There are already some reports of TCOs in Asia, Africa, and Latin America actively engaged in politics, sponsoring or co-opting government officials who can give them free reign to conduct their illicit activities. TCOs are also providing critical social and philanthropic services and employment opportunities to local populations in the absence of the state. Pablo Escobar, notorious head of the Medellin cartel and Colombian politician, was an early example of the criminalized state and philanthropic practices funded by drug money in the 1980s. In a 2012 article, Moises Naim described cases in which not only did the government have ties to organized crime, but also its officials, police, and/or military actually took part in illicit enterprises; Guinea-Bissau is a current example of a mafia or narco-state.[12]

As TCOs evolve in the future, the concept of a "criminal state" will be an important one if TCOs elect to complement their pursuit of profits with actual power. Michael Miklaucic and Moises Naim describe the notion of the criminal state as a spectrum of characteristics: state penetration, infiltration, and capture. At one end of the spectrum is "criminal penetration," which occurs when an illicit network, be it criminal, terrorist, or insurgent, is able to place "one of its own" into the state structure. That agent may conduct formal functions on behalf of the state but also carry out actions in support of an illicit network or criminal enterprise. "Criminal infiltration" occurs when the infection has spread throughout the state apparatus within the given country. "Criminal capture" constitutes the condition of dysfunctional governance in which criminal agents are so sufficiently prominent in positions of state authority that their criminal actions cannot effectively be restrained by the state.[13] The "criminal state" model could be the future trajectory for some TCOs that will further empower them and threaten global security.

The Convergence of Terrorism and Crime

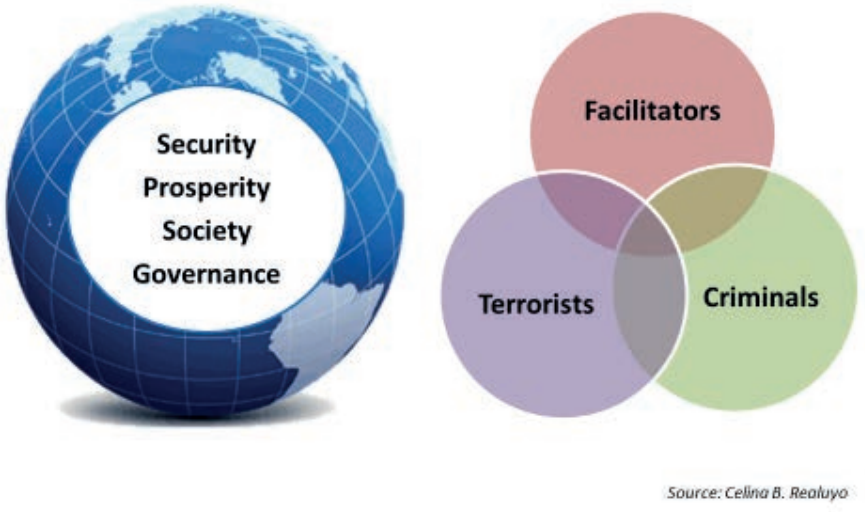
The convergence of TCOs and foreign terrorist organizations (FTOs), reflecting the intersection of normally distinct types of illicit organizations, has become a growing global security concern. Traditionally, organized crime was considered a public security problem and was addressed by state and local law enforcement authorities. Terrorist and insurgent groups were regarded as armed groups with political aspirations, including regime change that directly threatened the sovereignty of the nation-state. These illicit actors actively seek out governance gaps, socioeconomic vulnerabilities, and character weaknesses as openings to conduct their nefarious activities and expand their power and influence throughout the world. With globalization, terrorists and criminals groups have internationalized their support and operations and brokered

[11] Beittel J.S., Mexico's Drug Trafficking Organizations: Source and Scope of the Violence. Congressional Research Service Report for Congress. http://fas.org/sgp/crs/row/R41576.pdf. April 15, 2013.
[12] O'Regan D., Narco-States: Africa's Next Menace. *The New York Times*, March 12, 2012. www.nytimes.com/2012/03/13/opinion/narco-states-africas-next-menace.html?_r=0.
[13] Miklaucic M., Naim M., The Criminal State. In: Miklaucic M, Brewer J, eds. *Convergence: Illicit Networks and National Security in the Age of Globalization.* Washington, DC: NDU Press; 2013.

formidable alliances, and they now present complex transnational threats that put security and prosperity at risk around the world (see figure 2).

After the fall of the Berlin Wall, many terrorists lost state sponsorship, namely from the Soviet Union, and were forced to turn to crime to maintain themselves and promote their agendas. Organizations that represent this dangerous convergence of terrorism and crime include the Haqqani network in Afghanistan and Pakistan, FARC in Colombia, Shining Path in Peru, al Qaeda in the Islamic Maghreb in North Africa, and Lebanese Hezbollah. Hezbollah is considered perhaps the best organized and most business-savvy terrorist organization that relies on global facilitators engaged in narcotics, arms, and counterfeit trafficking and money laundering for financing and support. To address the convergence of terror-crime networks, governments need to engage in more cross-border collaboration among military, intelligence, and law enforcement agencies to better understand and combat illicit networks.[14] Going forward, as TCOs become more wealthy and pervasive, they may seek actual political power and transform into politically driven organizations that will directly challenge the nation-state.

Figure 2. The Convergence of Terrorism and Crime: A Threat to Sovereignty



Implications for Future Military Operations

As TCOs become more powerful and present a greater threat to state sovereignty, U.S. national security strategy will have to directly address them. TCOs are evolving into a formidable adversary as they are better financed, armed, and staffed than public security forces in many parts of the world. They are very versatile organizations that constantly capitalize on new market opportunities and seek to circumvent state countermeasures. In remarks at the Atlantic Council's "Disrupting Defense" conference in May 2014, Chairman of the Joint Chiefs of Staff General

[14] Realuyo C.B., The Terror-Crime Nexus: Hezbollah's Global Facilitators. *PRISM.* 2014; Vol. 5, no. 1, 116–129.

Martin Dempsey outlined his "2-2-2-1" strategic concept, focusing on specific current and emerging national security threats to the United States. It comprises two heavyweights that will influence our future strategy, Russia and China; two middleweights, North Korea and Iran; two networks, al Qaeda and *transnational organized crime from our southern hemisphere*, and one domain, cyber. He stated, "*Those things have influenced, are influencing me today and will influence you in the future. One of them or more.*"[15] General Dempsey recognizes TCOs as a clear and evolving threat to U.S. national interests; he noted that new tools are required for dynamically managing a more complex security environment but shared his fear that we will not innovate quickly enough for new challenges given current budget constraints.

If tasked to combat TCOs, the Joint Forces must understand this unconventional adversary in depth. TCOs are non-state actors that are difficult to identify due to their networked nature. They do not wear uniforms, do not have traditional command and control structures, and do not respect borders or human rights. The Joint Force must recognize their critical enablers, vulnerabilities, and motivations to better detect, disrupt, dismantle, and deter the TCOs that threaten U.S. security and prosperity. The Joint Force will have to expand its collection and use of intelligence to identify, target, and attack these transnational criminal networks through more creative kinetic and non-kinetic military operations as circumstances warrant.

As John Arquilla at the Naval Postgraduate School has said, "*It takes a network to defeat a network,*" and the Joint Force will have to build an effective one to combat transnational criminal networks. Arquilla and David Ronfeldt recently expanded their description of an effective network-building process:

- The network's narrative is the story that draws people to the network and keeps them in it, even in the face of adversity.
- Its social basis brings together actors from diverse places and makes the network the focus of their loyalty.
- The doctrine or concept of operations employed—from mass popular movements like the Arab Spring to insurgents and, increasingly, even conventional traditional military operators—is to "swarm."
- Technological "kit" is the final foundational element to which network-builders should be attentive. It is crucially important that a network's communications be capable of great throughput, but with a high level of security. But even with the availability of high throughput, secure communications will prove ineffective if the organizational design of a network is vertically (that is, hierarchically) rather than horizontally oriented to maximize linkages among the many small nodes that form the best networks.[16]

These factors will need to be incorporated by the Joint Force and the broader U.S. Government to build the best networks to combat TCOs. The agility of transnational criminal networks to respond to and outmaneuver government countermeasures will require a Joint Force with the

[15] Dempsey M., Gen. Dempsey's Remarks and Q&A at the Atlantic Council's Disrupting Defense Conference. May 14, 2014. http://www.atlanticcouncil.org/events/past-events/dempsey-calls-for-innovation-in-defense
[16] Arquilla J., To Build a Network. *PRISM.* 2014; Vol 5, No. 1 22–33, available at: http://www.ndu.edu/Portals/59/Documents/CCO/PRISMVol5No1.pdf

ability to analyze TCOs, understand their incentives, identify their vulnerabilities, and design courses of action to mitigate their impact on national security.

Under the current legal authorities in the United States, civilian law enforcement agencies have the lead in pursuing, arresting, and prosecuting transnational organized crime. The Department of Defense and U.S. Armed Forces are authorized to support law enforcement agencies pursuant to U.S. Code Title 10, Chapter 18.[17] Much of that support is in monitoring and detection activities rather than interdiction itself; interdiction and prosecution are the purview of law enforcement agencies and the Departments of Homeland Security and Justice. In combating transnational organized crime, the military plays a critical role in gathering intelligence and supporting law enforcement operations in the counter-narcotics arena. The Office of the Deputy Assistant Secretary of Defense for Counter-narcotics and Global Threats directs Department of Defense (DOD) counterdrug activities and oversaw a budget of $1.37 billion in fiscal year2013. These funds support local, state, Federal, and foreign law enforcement agencies to diminish the national security threats caused by the drug trade. DOD provides unique military platforms, personnel, systems, and capabilities to support Federal law enforcement agencies and foreign security forces involved in counterdrug missions. A key aspect of this program is the focus on increasing partner nation capability to combat narcotics trafficking worldwide.[18] Given the growing national security threat from TCOs beyond the drug trade, some advocate the expansion of DOD authorities for military involvement in combating transnational organized crime. DOD and the military possess far greater resources than civilian law enforcement agencies that could be better applied in the fight against transnational organized crime.

The whole-of-government approach adopted in the wake of the tragic September 11, 2001, attacks has led to more effective interagency collaboration among military, intelligence, and law enforcement circles on national security issues like terrorism. However, as our adversaries, including TCOs, become more powerful and quickly adapt to their environment, the U.S. Government must broaden its definition of national security threats and enhance all agency authorities and abilities to combat transnational organized crime. The Joint Force must prepare itself to face multifaceted and complex security threats such as those posed by TCOs. The United States should strive to harness all resources available to combat transnational threats like transnational organized crime and terrorism. Transnational organized crime can no longer be regarded as a task solely for law enforcement to tackle but rather a national security threat to the sovereignty, economy, and citizen security of the United States and its allies.

[17] Department of Defense (February 2014). Department of Defense Instruction 3025.21. *Defense Support of Civilian Law Enforcement Agencies*. www.dtic.mil/whs/directives/corres/pdf/302521p.pdf.
[18] Logan E., Statement for the Record before the Senate Caucus on International Narcotics Control: Future Counternarcotics Efforts in Afghanistan. January 15, 2013. www.drugcaucus.senate.gov/hearing-1-15-14/DOD%20Erin%20Logan.pdf.

References

Arquilla J., (2014). To Build a Network. *PRISM* , 5 (1), 22-23. http://www.ndu.edu/Portals/59/Documents/CCO/PRISMVol5No1.pdf

Beittel J.S., (2013). *Mexico's Drug Trafficking Organizations: Sources and Scope of the Violence.* Congressional Research Service Report for Congress. http://fas.org/sgp/crs/row/R41576.pdf.

Department of Defense Instruction 3025.21. (2013). *Defense Support of Civilian Law Enforcement Agencies.* http://www.dtic.mil/whs/directives/corres/pdf/302521p.pdf

INTERPOL. Cybercrime. www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Logan E., (2013). Statement for the Record before the Senate Caucus on International Narcotics Control, Future Counternarcotics Efforts in Afghanistan. www.drugcaucus.senate.gov/hearing-1-15-14/DOD%20Erin%20Logan.pdf

Miklaucic M., and Brewer J., (eds.). (2013). *Convergence: Illicit Networks and National Security in the Age of Globalization*. Washington, DC: NDU Press.

National Security Council. (2011). *Strategy to Combat Transnational Organized Crime.* https://www.whitehouse.gov/sites/default/files/Strategy_to_Combat_Transnational_Organized_Crime_July_2011.pdf

O'Regan D., (2012). Narco-States: Africa's Next Menace. *The New York Times*. http://www.nytimes.com/2012/03/13/opinion/narco-states-africas-next-menace.html?_r=0

Realuyo C.B., (2014). Hezbollah's Global Facilitators in Latin America. Testimony at a hearing entitled: Terrorist Groups in Latin America: The Changing Landscape. Subcommittee on Terrorism, Non-Proliferation, and Trade, House Committee on Foreign Affairs, U.S. House of Representatives. http://docs.house.gov/meetings/FA/FA18/20140204/101702/HHRG-113-FA18-Wstate-RealuyoC-20140204.pdf

———. (2014). The Terror-Crime Nexus: Hezbollah's Global Facilitators. *PRISM*. 2014; Vol. 5, no. 1, 116–129. http://www.ndu.edu/Portals/59/Documents/CCO/PRISMVol5No1.pdf

Texas Department of Public Safety. (2014). *Assessing the Threat of Human Trafficking in Texas.* https://www.dps.texas.gov/director_staff/media_and_communications/2014/txHumanTraffickingAssessment.pdf

The White House. (2010). *National Security Strategy of the United States.* https://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf

Uplinking into the Future: Education in 2030

Paulette Robinson,[1] *Mitch Armbruster, and Hannah Snapp*

The educational landscape, both civilian and military, will change significantly in the coming years. These changes will be driven by several factors. First, changes in the developing world, specifically economic development, will change worldwide demand for education. New educational techniques will change the learning experience, both in and outside of the classroom. Rapid technological advances have the potential to radically upend the current learning infrastructure.

This paper will present several educational developments, some of which are quickly being absorbed into the mainstream, and others that are currently on "the edges" of the formal educational system. There are several possible outcomes – anything from small incremental modifications to a complete upending of the way we approach learning. This paper will look at both changes currently underway and also speculate on what the future of education could possibly look like. These predictions present several possibilities for what education will be in 2030, along with developments that could take education and training in unpredictable directions.

Demographic, Economic, and Political Shifts

According to the United Nations (UN) Population Fund, the vast majority of world population growth over the next decade will be in the developing world. Using the UN Population Fund's medium variant estimates, by 2025 the world's population will rise to an estimated 8.1 billion people, up from approximately 7.1 billion in mid-2014. Population growth is projected to continue in the decades afterwards as well, up to approximately 9.6 billion in 2050 and 10.9 billion by 2100. Most of this growth will be in what is now referred to as the developing world; almost all of the additional 3.7 billion people in the world of 2050 will live there. In fact, population growth rates over the next four decades will be seven times greater in the developing world than in the developed countries of Europe and North America.[2]

Analysts predict that the world's population will continue to move to cities. As of 2014, more than half of the world's population lives in cities, the highest percent in history.[3] Increased urbanization, especially in the developing world, will create new issues to which governments and nongovernmental actors will have to adapt. According to the UN Department of Economic and Social Affairs, increased urbanization means that "*managing urban areas has become one of the most important development challenges of the 21st century.*"[4]

---

[1] robinsonp@ndu.edu

[2] United Nations Population Fund. *World Population Prospects*. New York: United Nations; 2013

[3] World Health Organization. Global Health Observatory. Urban population growth, 2014. www.who.int/gho/urban_health/situation_trends/urban_population_growth_text/en/.

[4] United Nations Department of Social and Economic Affairs. World's population increasingly urban with more than half living in urban areas. July 10, 2014. www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

In 1980, urban areas with a population over one million housed only 13 percent of the world's population. In 2014, over 22 percent of the world's population lives in urban areas with more than one million people. This number is expected to rise to 27 percent by 2030 of the world's population is expected to live in urban areas of more than one million people by 2030. Overall, more than half of the world's population will live in some type of urban area.[5] One of the most prominent changes in the urban environment is the rise of the megacity, cities with over 10 million in population. The growth of megacities will pose major challenges for US and world security (Bartone and Sciarretta, 2015, this volume). The vast majority of urbanized growth has been, and will continue to be, in the developing world. A demographic shift on this scale will continue to produce significant new problems in public health, national and transnational crime, security, and economics.[6] As the global center of population rapidly shifts to the developing world, all major U.S. institutions, from military to healthcare to education, will need to respond.

Changes in global economic conditions over the next several decades will also prove disruptive. Much like expected demographic and urban transformations, the developing world will be at the forefront of the changing global economy. By 2025, the World Bank estimates that the majority of worldwide economic growth will be generated in the developing world.[7] Overall, developing states recovered from the economic dislocation of 2008–2009 relatively quickly, returning to their previous high growth rates. By contrast, the developed world struggled to regain its footing after the most acute period of the global economic crisis, and more than half a decade after the collapse, economies across the developed world remain weak.[8] As the economies of the developing world afford their citizens greater affluence, those economies themselves will become more important through their increased purchasing power, driving demand for education.

The demographic and economic transformations that the world will undergo over the next several decades will also alter the political and strategic landscape. As the developing world continues to grow demographically and economically, its political importance will increase dramatically as well. While the states of the developing world will grow more powerful and politically relevant, the established powers of the developed world will begin to take more of an interest in areas of the world they formerly considered peripheral. Developed nations' interest in the developing world as an emerging economic powerhouse will drive political and economic engagement.

How will education change over the coming decades? What will the world of education look like in 2030? Much like the demographic, economic, and political changes that the world is currently experiencing, major transformations in education are under way. These developments in education will interact with the other major worldwide trends, producing a strategic environment that is much different than the one the United States currently inhabits. New approaches and

[5] Ibid.
[6] Norris F., For Biggest Cities of 2030, Look to the Tropics. *The New York Times*, July 11, 2014. http://www.nytimes.com/2014/07/12/business/for-biggest-cities-of-2030-look-toward-the-tropics.html
[7] World Bank. *Multipolarity: The New Global Economy*. Washington: World Bank; 2011.
[8] Ibid.

innovations will be paired with cutting-edge technologies to spread personalized educational opportunities farther and wider than ever before.

Trends in Teaching Methods and Techniques

Several educational innovations are currently disrupting and reshaping the way we teach and learn. Advances in technology and pedagogy will allow teachers and institutions to customize educational methods, assessments, and desired outcomes for individual students. The changes currently underway in education are diverse, but the general theme that unites all of them is personalized learning.

At its broadest level, personalized learning offers individual students the opportunity to shape their own learning through use of new approaches and new technologies. Colleges and universities have started supporting personalized learning through the use of learning data keyed on each student. The data provides students with recommended courses, as well as updates to program, project, and course progress. Institutions can monitor student progress for advisement and institutional metrics of value that could include staff performance, budget and financial health, student retention and graduation rates, and so forth through online dashboards. Some states offer state-wide educational e-portfolios that can collect not only transcripts from courses, but also student learning artifacts that follow students through their educational pursuits. These artifacts help facilitate learning by highlighting student strengths and weaknesses and can allow students to make better choices about their own education. Personalized learning will evolve to meet the needs, interests, and ambitions of individuals both in and outside of traditional educational environments.

While personalized learning has always been with us in terms of lifelong learning, data-driven approaches are dominated by educational institutions. However, individuals are increasingly able to take charge of their own education through alternative forms of learning. At the kindergarten through 12th-grade levels, home schooling has offered latitude for parents in tailoring their children's education. Parents have self-organized to expand their curricula to shared courses amongst their children. In some cases, local schools have allowed home-schooled students to drop in for courses when a class requires lab equipment or more specialized knowledge in order to enhance their educational experience. A large number of parents have paired their children with mentors in their areas of interest to further enrich their student's education. Mentorship allows parents and students to leverage the human resources in their communities to personalize and advance their educations. Like other educational innovations, the increase in home schooling has been enabled by technological advances that allow information to be more widely distributed at a lower cost.[9]

Across higher education, programs that allow students to create their own multidisciplinary majors are becoming increasingly popular, if still relatively rare. Most higher education institutions primarily offer more traditional degree and certificate programs where most coursework and learning outcomes are predetermined based on students' age for everyone. As personalized education becomes more of an expectation among students and teachers, the

[9] Andrade A., *An Exploratory Study of the Role of Technology in the Rise of Homeschooling*. Ohio State University; 2008.

exclusive role of colleges and universities will change. Shared credit between higher education institutions will be more flexible and inclusive, leveraging the strengths and expertise of their faculty regionally and globally breaking down exclusive programmatic requirements and business models.

Competency-based education offers students a more individualized approach from traditional curriculum assessment requirements. While still tied to an institution, students enrolled in competency-based educational programs are required to demonstrate a competency or skill rather than achieve a grade. Competency-based education reduces the time needed to earn a degree and allows students to tailor their learning to specific requirements or skills of employers. This approach helps develop particular skill sets and abilities through projects and specific tasks, tracking student progress from point A to B through their knowledge acquisition.[10] Using this more personalized approach, students can develop competencies more broadly in and outside of traditional institutions.

The traditional role of higher education institutions as assessors of knowledge may shift to outside brokers supported by employers and learners. These changes disaggregate institutions' instruction and learning from assessment, giving students more freedom to create their own learning program of study. Students will be able to learn from multiple models that include courses, games, mentorship, communities of interest, etc. gaining competencies relevant to the student and their personal aptitudes. This approach calls into question the certifying business models and values of educational institutions. It's likely that traditional educational institutions will no longer require students to exclusively study with them to gain certification. Faculties have begun, in some cases, to establish their own brands that are not exclusively tied to the institution.

This trend is likely to accelerate in the near future. Certifying institutions will be concerned primarily with guiding students to broad learning resource options that go beyond their own particular institutions. Schools would then assess student competencies and match them with appropriate employers or help them select further educational opportunities. The business model serves both students and employers like a matchmaker offering a consolidation and brokerage of learning experiences and competency evaluation. Like the institutions they inhabit, educators will also be able to shift from dispensing knowledge to mentoring and facilitating regardless of institutional affiliation. This faculty model is evident in educational institutions using adjunct faculty who often teach at a number of institutions.

Advances in online and mobile education will continue to allow students to personalize their educations, both by prioritizing avenues to pursuing the competencies they need and freeing them to engage in learning events remotely and at a time of their own choosing. Mobility and online learning are complementary trends. Both are currently altering the traditional "brick and mortar" approach to education. Students can access information from any place in the world and at any time. Methods of acquiring competencies can range from more traditional courses, to

[10] United States Department of Education. Competency-Based Learning or Personalized Learning. http://www.ed.gov/oii-news/competency-based-learning-or-personalized-learning

multiplayer games, communities of interest collaboratives, virtual labs, virtual worlds simulations, etc.

An older model of education took place primarily inside of a classroom – faculty delivered information to students, engaged them critically in various ways to help them further grasp the information, and then assessed their knowledge of that information. Online and mobile education allows for much of the delivery of information to take place outside of a classroom – students can have information delivered to them in a way that best suits them. Faculty can assist with information delivery to students, but delivery would take place primarily outside of the classroom. This development is strongly linked with the overall trend of personalization in education. Students are able to customize how they will receive information. For some students, this will likely continue to be reading traditional books and papers. Others, however, will be able to utilize increasingly advanced online based multimedia that will better suit their learning goals. Technological advances are helping researchers and educators understand how students learn, and some of these advances will be explored later in this paper.

If predictions about global trends in demographics and economics prove accurate, the developing world will become increasingly important, and demand for education in the developing world will rise dramatically. Online and mobile education can offer the most efficient and cost-effective way to deliver educational in the developing world. While physical infrastructure is often acutely lacking in large parts of the developing world, access to the internet, primarily through mobile platforms such as cell phones, is quite comprehensive. For example, there are currently more than twice as many cell phone users in Africa than there are people in the United States.[11]

One of the most innovative and discussed online learning platforms are Massive Open Online Courses (MOOCs). These internet-based courses can enroll thousands of students at a time. MOOCs leverage online learning without the business model of tuition on a massive scale. While the design and delivery of MOOCs are constantly evolving, the option of packaged information available to anyone from experts in the field has captured those who have an interest in personalized learning rather than fulfilling a prescribed curriculum to complete a degree program.[12]

MOOCs, or something similar to them, have enormous potential to improve DoD training and education. With service members spread around the globe, often in remote places with little in the way of traditional military education, MOOCs and other online educational tools have the potential to open up educational activities to service members while they are in the field. Connection via the internet, either on a computer or a mobile device, can allow military personnel to access specialized training as they need it. Not being constrained by a traditional

[11] Yonazi E., Kelly T., Halewood N., and Blackman C., *The Transformational Use of Information and Communication Technologies in Africa.* Washington, DC: World Bank; 2012. http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:23262578~pagePK:210058~piPK:210062~theSitePK:282823,00.html

[12] Lushnikova N., Chintakayala P.K., Rodante A., Massive Open Online Courses from Ivy League Universities: Benefits and Challenges for Students and Educators. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2254132&rec=1&srcabs=2350964&alg=1&pos=2

educational framework, such as a syllabus or prescribed course of study, a service member can access training to acquire skills they need on the spot.

As MOOCs continue to become more accepted as a legitimate alternative to physical classroom instruction, certification and degree programs that use MOOCs will become increasingly common. Georgia Tech is the first prominent university to offer a degree program that can be completed solely via MOOCs. The program, a master's degree in computer science, received twice as many applicants as the comparable traditional computer science graduate program at Georgia Tech. At $6,600 total for the MOOC-based degree, the program is significantly more affordable than the traditional classroom-based degree, which costs approximately $44,000.[13]

Critics of MOOCs point out that they tend to have high failure and dropout rates compared to not only traditional classes, but also to online courses as well.[14] While it is unlikely that MOOCs, or something like them, can be a substitute on their own for more traditional educational methods, MOOCs can be an important part of a competency-based system where students pick and choose content that reinforces their personalized learning plans. Many courses have components that a student may want to study, without the need to complete the course. While exactly where MOOCs will fit into the arena of higher education is still being explored and experimented with, it is likely that instructional platforms that can accommodate massive numbers of students outside of an institutional affiliation will be a factor in the near term future of personalized and competency-based education.

MOOCS are not the only educational method that can be mined for the future. Many of these new methods are possible due to technological advances or the widespread adoption of existing technology. Though these new approaches differ methodologically, they all have the effect of personalizing education to better fit student needs and goals.

The flipped classroom upends the traditional model of education while still working within the traditional environment. In a flipped classroom, students do their problem sets and "homework" in class, and watch recorded lectures and other appropriate videos (such as "Kahn Academy," documentaries, and other assignments) at home. This allows teachers to assist students with their work in a way they have been unable to do in a traditional classroom. Flipped classrooms give instructors unprecedented time to devote to helping students work through problems rather than relying on them to solve the problems at home.[15] Students that need more time with instructors can benefit greatly by having teachers who work through problems with them in person before assignments are due. While the technology is not new, the widespread adoption of the internet opens a space for more and more students to take advantage of this new technique.

One of the more experimental and innovative approaches to education offered in a physical space is being pioneered at the new Ecole 42 in France. The Paris-based school, founded by French

---

[13] Belkin D., First-of-Its-Kind Online Master's Draws Wave of Applicants. *Wall Street Journal*. October 29, 2013. http://www.wsj.com/articles/SB10001424052702304470504579166112833252206.
[14] Parr C., MOOC completion rates below 7%. *Times Higher Education.* May 9, 2013. http://www.timeshighereducation.co.uk/news/mooc-completion-rates-below-7/2003710.article
[15] Tucker B., The Flipped Classroom: Online instruction at home frees class time for learning. *Education Next*. 2012. 82–83. http://educationnext.org/the-flipped-classroom/

billionaire Xavier Niel, has no teachers, books, tuition, labs, student centers, or almost anything that is normally associated with a higher education. In fact, the school even lacks specific courses. Instead, the entire student body, between 800–1,000 students per year, works in a single building housed in the middle of Paris. Students are given coding challenges that must be completed as part of a team. All projects are collaborative, and students must turn to each other, rather than to instructors, for assistance. The challenges increase in difficulty as students advance through the program. The school does not charge any tuition, and students can complete the program in 2 or 3 years.[16]

Disruptive Technology in Education and Training

While technology has been integrated into new approaches to education such as flipped classrooms and MOOCs, more technologically intensive education methods will further disrupt traditional education. Driven by both technological advances and the pressures of budget cuts, bloated administrations, and increasingly prohibitive costs, these changes have the potential to radically reform education. At a minimum, these technologies and pressures are forcing educational institutions to change their approaches and business models to adapt.

Experiential and immersive technologies are slowly making their way into traditional education as a mainstream approach to teaching and learning. Gaming, 3–D virtual worlds, online scenarios, simulations, interactive role playing, modeling, and online apprentices are all ways for students to apply what they are learning through problem-solving, critical thinking, and creating.[17] Approaching learning through these techniques puts the student at the center of the learning experience with the faculty as a guide or mentor, asking critical questions and guiding students to resources. Students are encouraged to be creative and innovative with their solutions to complex problems that are designed to have multiple answers.

Various types of high-tech learning spaces are emerging and will continue to provide students with new options. Technology will be integrated more fully into traditional classrooms as teachers adapt to new technologies and institutions compete for student enrollments. Students expect high-tech access. Studio-style learning spaces, where learning is primarily accomplished via peer-to-peer interaction with faculty facilitation, are growing as a best practice. This learning model demonstrates how corporation like Microsoft and IBM have underwritten educational innovations for its clear resourcing benefit. More collaboration between institutions will be common as the boundaries between academia, industry, and students become more fluid. Finally, virtual spaces that can be tailored to almost any imaginable group of students or scenario will allow students to robustly interact within various environments at a low cost. As the developing world demands more education in tandem with increased economic growth and worldwide demands for skilled workers, virtual education will be a cost-effective way to provide cutting-edge training.

---

[16] Tweney D., This French tech school has no teachers, no books, no tuition — and it could change everything. *Venture Beat.* June 13, 2014. http://venturebeat.com/2014/06/13/this-french-tech-school-has-no-teachers-no-books-no-tuition-and-it-could-change-everything/

[17] McClarty K.L., Orr A., Frey P.M., Dolan R.P., Vassileva V., McVay A., A Literature Review of Gaming in Education. *Pearson Report*. 2012

Gamification and digitized learning environments will become prevalent as the cost of the underlying technology falls, the capabilities become more sophisticated and intuitive for learners to achieve targeted competencies. Other forms of advanced technology will also become standard learning approaches. 3–D printing, object-embedded intelligence, and the "internet of things" will make learning spaces more interactive and provide real-time relevant data.[18] Maker spaces and traditional classrooms will seamlessly combine online learning with physical application, allowing students to access the best of information technology while working with peers on collaborative projects.[19]

Advances in gaming and simulations are of special interest to military education. Online gaming and simulations can bring in students and instructors from around the world, allowing participation on previously unimaginable scales. Not only does this allow more students from geographically dispersed regions take part in educational activities, but it allows for sharing of information and expertise on a much larger scale than previously possible. This diversity of expertise and interests allows students to learn from each other, not just instructors.

Virtual and augmented realities will allow students to practice and improve a vast array of skills not only with increasing realism and utility, but also at a time convenient for them. Freed from the need to be physically present at an educational institution, students will experience flexibility to pursue personalized learning goals. Technical fields such as medicine and engineering where hands-on repetition is crucial will benefit from virtual and augmented realities.[20] Virtual reality systems such as Oculus Rift can create a rich immersive platform for learning. Augmented realities are a hybrid environment where the participant interacts with the physical world, with additional information being provided by a heads up display. This interaction is "augmented" through the use of virtual reality components such as 3–D displays, sound effects, personalized annotation, photography, and other interactive components that can be added or modified by instructors and students. The result of introducing both virtual and augmented reality into education is to create a far more enriching environment. Collaboration, shared learning, and distance learning will all be greatly enhanced through the use of virtual and augmented realities.[21]

Big data has the potential to change the teaching and learning landscape in ways that have not been possible in the past. Applying big data to teaching and learning will be the engine that drives personalized learning portals; each individual will have a better understanding of his or her performance on multiple competencies. Access to—and ability to understand—this information will also allow students to use global resources to improve performance. These can be adjusted based on the individual student's interest, aptitude, health, and the needs of employers.

---

[18] Zappa M., Envisioning the Future of Education Technology. June 2014. http://www.envisioning.io/education/

[19] For an example of a creative space using 3–D printing, see the MakerBot Academy. http://www.makerbot.com/faq/

[20] Parr C., The Future of Higher Education? Five Experts Give Their Prediction. *Times Higher Education*. March 2014. http://www.timeshighereducation.co.uk/the-future-of-higher-education-five-experts-give-their-predictions/2011867.article

[21] Canbeck N.G., J. Hargis, Connecting Augmented Reality to Higher Education: Mash-Up. *International Association for Technology, Education and Development (IATED) Proceedings*, July 2011.

Big data will contribute in critical ways to learning science, helping educators, parents, and students all better understand and take advantage of how learning takes place. Until recently, most education data sets have been too small to fully understand how people learn. With the onset of large data sets, tailored algorithms, and visualization tools, the education community will be able to provide real-time and effective personalized learning environments. Adaptive learning technologies are an example of how learning can be tailored based on big data. For example, the Khan Academy is using adaptive learning tools to teach a wide variety of mathematics online. Their tools are able to administer just-in-time lessons to inform gaps in assessment, iterate problems tailored for the individuals learning needs, and move the students through the learning process from simple to complex math skills.[22]

One form of data that will help inform learning will be the enormous amount of information generated by advanced neuroscience technologies and techniques. Advanced neuroscience technologies not only will allow scientists to monitor and understand when the brain is signaling readiness to learn a particular skill, but also will inform us as to how to stimulate and augment areas in the brain to enhance learning.

The "internet of things"—devices that are constantly reporting data to the cloud from wearable devices and sensors—will enhance education science in new and significant ways. Soon, it will be possible to monitor sleep, exercise, heart rate, emotions, and so forth in order to understand the impact of the whole person on learning. Optimizing learning will not be limited to information and assessment. In addition, sensors will become ubiquitous in our environment, providing a deluge of data that can be used in student research projects and original contributions to the world's body of knowledge.

There are several possibilities for how these trends will change the current system of education, both civilian and military. While no one can predict the future, several possibilities can be considered along a spectrum of plausible outcomes. On one end of the spectrum is an educational infrastructure similar to what exists today. New technology and teaching methods will supplement the existing education system. Most institutions will continue to operate as they do now, with only minor changes. On the other end of the spectrum is a radically changed education system with little in common with today.

If information delivery becomes no longer required as the primary activity for teachers, how will classes need to change and adapt? Are educational events, such as classes and lectures, necessary when access to information is readily available? Faculty roles may become similar to mentors who guide students, rather than simply conveying information. In the future, what constitutes "faculty" may include a much broader set of individuals across a range of age and expertise. Social media and communications technology will allow students to leverage the knowledge and expertise of members of their community outside of educational institutions. Everyone will be teacher.

[22] Khan Academy. About. https://www.khanacademy.org/about

Long Term Possibilities

Looking beyond the immediate future, advances in education technology have the potential to totally recreate the entire educational system. One way to imagine the difference between the previous changes and the longer term ones is to think of the short-term changes as "disrupting" the educational landscape and the long-term changes as "revolutionizing" it. These long-term technologies have the potential to absolutely rupture our entire process of learning. How will these over-the-horizon technologies shape education?

What is the future prognosis for educational institutions themselves? Will educational institutions as we know them exist by 2030? If not, how will society continue to equip individuals with these three general capabilities?

Predicting the future, especially when concerning advanced technology, is an inherently difficult proposition. Simply consult the predictions of flying cars and colonies on the moon to see how forecasting can go awry. However, it is possible to make a number of projections based on the current trends in technology related to education and information. These are possibilities for the future of learning that could revolutionize the field if they come to pass.

There are several advanced educational technology scenarios that are entirely realistic. One possibility for beyond 2030 could easily include direct brain input of information. In this future, information is downloaded from a computer directly into a person's brain. These capabilities are currently evident as augmentations to guide prosthetics. Brain-to-brain transmissions are already being successfully piloted.[23] Connected to a wireless network, young children will be monitored for neuro-readiness and information will be delivered at the optimal time.

This technology could extend beyond children. Warfighters in the field could receive just-in-time mission information that will allow them to act in sync with other warfighters and networked equipment. Optimal information uploads will be determined by precise personalized data. There will be no need to seek out information and use inefficient methods of attempting to learn and retain; all the information needed will be instantly available. Nicholas Negroponte posits yet another method for instantly attaining information. He suggests that we will be able to ingest information using small capsules, similar to medicine.[24]

Learning scaffolds, taxonomies, and structures will come with information to assist in the organization of the facts for efficient retrieval, use and application. The larger question that would need to be examined is: Who determines the scaffolds for the uploaded information? Examples of how to efficiently use information will be uploaded as a basis for building expertise. Educational institutions will no longer be required to deliver information; it will be as ubiquitous as air. What will be the focus if information delivery is no longer required?

---

[23] Grau C., Ginhoux R., Riera A., et al. Conscious Brain-to-Brain Communication in Humans Using Non-Invasive Technologies. *PLOS One.* August 19, 2014. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4138179/

[24] Negroponte N., A 30-Year History of the Future. *Technology, Entertainment, and Design*. March 2014. https://www.ted.com/talks/nicholas_negroponte_a_30_year_history_of_the_future?language=en.

Individuals will be augmented with implanted chips to enhance learning and processing of information. These implants will enable individuals to electronically interface with not only computer systems, but directly with other people as well. What one learns as an individual instantly becomes the learning experience of everyone connected to a network. It is crowd-sourced thinking at the level of the brain. This will lead to almost unimaginable growth in social learning, where individuals learn directly from one another rather than through a third party such as a school. Communication will be triggered using the body and mind, rather than an external device.[25]

Experiential and immersive learning will take a variety of forms. Through triggers in the brain, individuals will have the ability to immerse themselves in a 3–D virtual world, the real world, or both simultaneously. Through sensor information tied to the internet of things and data stored in a cloud network, these worlds will be rendered based on real data. Imaginary or creative designs will be visualized and then rendered. Designs will be prototyped using 3–D print technologies from blueprints updated on the fly shaped totally within an individual's thought process. We will be able to reinvent who we are and collaborate easily and immediately with anyone.

Problems will be embedded in particular virtual world contexts and presented to students to solve. All student actions will be monitored in robust data collections, adjusted to student responses and learning needs, and with progress reported into individual learning portals. Students will determine who has access to their learning data. It will no longer be owned and controlled by the institution certifying the data. Students of all ages will also have the opportunity to participate in creative maker spaces that will include members from several generations working and learning together to create, design, and manufacture new inventions or products. These spaces will be in communities with high-end 3–D printers, computing, and precision equipment. Virtual maker spaces will intersect physical spaces facilitating cloud resources and distribution of finished products. Age will not determine the teacher or mentor in these spaces; education will be a collective experience with each person respected for what they have to offer.

Mentor networks will link learners and those who are willing to offer their time as mentors. Mentorship capabilities will be authenticated by data, not age or credentials. Similar programs have already shown success in the business world.[26] Competency-based progression will allow everyone the opportunity to become an educator or mentor. The proof of their ability will be in their success in assisting learners to meet their competency goals. Teachers will become brands and collect online and geographical followings that will go beyond an institutional affiliation. Mentors will be able to create avatars that can represent the person at various stages of the mentoring process. Peer-to-peer networks will enable education to become much more innovative and dynamic, allowing everyone to contribute to their own and others' education as facilitators and mentors.

Educational institutions in this scenario would probably not disappear but rather transform their core functions. They will serve as the institutional structure that creates scaffolds, experiential

[25] Kurzweil R., *The Singularity is Near.* New York: Penguin Press; 2006.
[26] de Janasz S.C., Sullivan SE, Whiting V. Mentor networks and career success: Lessons for turbulent times. *Perspectives.* November 1, 2003.

learning environments, and assessments to verify educational attainment. Without the limited structures of age groupings, these schools will advance learners on readiness, ability, and competency. Age cohorts and structured lock-step curricula will give way to collaborative and flexible learning environments, tailored to the needs and interests of each student. Schools could create resource-rich and engaging environments, available for groups or individuals to integrate particular concepts and skills. Physical technological resources can be based out of schools, allowing individuals to have easy access to specialized learning technologies. Schools will provide hubs for teaching and mentoring. Traditional educational events like courses and lectures will be replaced by immersive experiences. Schools could serve as brokers that match employers with students based on competencies that fulfill skill requirements for particular jobs. But the role of broker could also easily move to an external agent or industry that would be an independent verifier of competencies.

Risks

One significant issue that could challenge policymakers in the future will be access to these new educational technologies. Those with the resources to augment and provide data-rich quality information for upload will have the advantage over those who do not have the resources. This could be particularly true for developing countries that contain large "youth bulges," with a significant percent of their population being young. A considerable divide could also arise not only between the developed and the developing world, but also within states. The investments in these changes are not only monetary, but also cultural. How can the future education system take advantage of technologies and new research on how people learn? How do we share those advantages with the global populations on which we may depend for labor in the future?

While cybersecurity has become an increasingly important concern, demand for it will skyrocket as the world becomes more networked and dependent on technology. The more advanced technology becomes, the more it will penetrate our lives, opening individuals, institutions, and entire countries to increasingly sophisticated cyber-attacks. It will be more focused on a hybrid of digital bio with future bio computing systems. Information security concerning education today primarily consists of preventing the theft of sensitive private information, such as grades and financial records. A computer virus that can be delivered to an individual's brain through technology interfaces ceases to become only a computer virus and becomes almost indistinguishable from a biological disease. In an environment where educational technology directly interacts with human biology, cybersecurity becomes a matter of life and death.

Implications for Future Military Operations

A military that is part of a lifelong learning culture with access to the world's knowledge instantly uploaded into their brain anywhere at any time is a superior force. Tied together into a "hive," this shared collective intelligence will provide a coherent and singular force that can act as one. Mission information, battle plans, and so on could be distributed completely and immediately to the entire unit. Direct group sharing of information of an ongoing mission would enable effective and efficient responses in the field based on immediate feedback of the battle conditions shared immediately with the larger collective force. The physical and mental conditions of all individuals in the military action would be known and could be adjusted when needed by direct brain stimulation.

Mission rehearsals could be created to encompass entire teams anywhere by using virtual worlds or avatar surrogates. Performance data and mission improvements would be carefully monitored through data tracking and analytics. Adjustments will be made in real time and mission challenges adjusted during rehearsals in response to actions by soldiers in training.

Military education, and Joint Professional Military Education in particular, is different from civilian counterparts in several aspects. Military institutions tend to place a greater emphasis on learning from practitioners, often active duty or retired military, than civilian schools. The war colleges in particular operate almost like professional schools in the civilian world.[27] Faculty at the war colleges have traditionally relied almost exclusively on lectures and small seminars, relying on the Socratic method for fostering debate and discussion. Many critics have alleged that this method does not adequately prepare students to think critically about an increasingly complex world.[28]

Advances in educational technology and teaching methods presented in this paper can allow students new and innovative ways to study pressing national security issues. Combining new educational innovations with social media platforms new, online war gaming programs allows students and faculty to work together solving problems. One example of this is the increasing popularity and usage of the Massive Multiplayer Online War Game Leveraging the Internet (MMOWGLI) war gaming platform throughout the DoD.[29]

---

[27] Lamb C., Porro B., Next Steps for Transforming Education at National Defense University. *Joint Force Quarterly*. 2005; Issue 76, 1st Quarter, pgs. 42-43. http://ndupress.ndu.edu/Media/News/NewsArticleView/tabid/7849/Article/12362/jfq-76-next-steps-for-transforming-education-at-national-defense-university.aspx.

[28] Ibid.

[29] Robinson P., Bartels E., Cordero G., Feltz L., Wendt V., Law R., NDU Massive Game Pilot Paper. Washington, DC: Center for Technology and National Security Policy Working Paper.

Conclusions

If the projections for world demographic, economic, and political changes prove to be accurate, then the world of military education will need to adapt to meet new challenges. Advances in educational technology and approaches will both be shaped by these changes and drive them. As the developing world becomes more important to the United States economically and as a source of labor, military education will increasingly look to address regional issues and problems. Content will be tailored to each individual situation, to deliver maximum usability. Through mining big data stored on the cloud, educators will be able to compare performance results and best practices in even the most remote environments.

Advances in education will not just respond to the world; they will shape and drive it. In the future, education will be global, instant, and connected. Will our cultural and social structures change rapidly enough to leverage a future where information is ubiquitous, but knowledge and wisdom may be the challenges of the system? All 650 million cell phones in Africa are potential learning platforms that citizens could leverage in order to improve their lives. A population that can rapidly become more educated and productive can also rapidly change the circumstances of their home society. Peer-to-peer learning platforms and philosophies will allow information to rapidly spread horizontally, removing a key role formerly held by educational institutions.

References

Andrade A., (2008). An Exploratory Study of the Role of Technology in the Rise of Homeschooling. PhD diss., Ohio State University.

Belkin D., (2013). First-of-Its-Kind Online Master's Draws Wave of Applicants. Wall Street Journal. http://www.wsj.com/articles/SB10001424052702304470504579166112833252206.

Canbeck N.G., Hargis J. (2011). Connecting Augmented Reality to Higher Education: Mash-Up. International Association for Technology, Education, and Development (IATED) Proceedings.

Grau C., Ginhoux R., Riera A., et al. (2014). Conscious Brain-to-Brain Communication in Humans Using Non-Invasive Technologies. PLOS One. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC4138179/.

de Janasz S.C., Sullivan SE, Whiting V. (2003) Mentor networks and career success: Lessons for turbulent times. *Perspectives*.

Kurzweil R., (2006). The Singularity is Near. New York: Penguin Press.

Lushnikova N., Chintakayala P.K., Rodante A. (2012). Massive Open Online Courses from Ivy League Universities: Benefits and Challenges for Students and Educators. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2254132&rec=1&srcabs=2350964&alg=1&pos=2

McClarty K.L., Orr A., Frey P.M., Dolan R.P., Vassileva V., McVay A. (2012). A Literature Review of Gaming in Education. *Pearson Report*. http://researchnetwork.pearson.com/wp-content/uploads/lit_review_of_gaming_in_education.pdf

Negroponte N., (2014). A 30-Year History of the Future. Technology, Entertainment, and Design. https://www.ted.com/talks/nicholas_negroponte_a_30_year_history_of_the_future?language=en

Norris F., (2014). For Biggest Cities of 2030, Look to the Tropics. The New York Times. http://www.nytimes.com/2014/07/12/business/for-biggest-cities-of-2030-look-toward-the-tropics.html

Parr C., (2013). MOOC Completion Rates 'Below 7%'. Times Higher Education. http://www.timeshighereducation.co.uk/news/mooc-completion-rates-below-7/2003710.article

Parr C., (2014). The Future of Higher Education? Five Experts Give Their Prediction. Times Higher Education. http://www.timeshighereducation.co.uk/the-future-of-higher-education-five-experts-give-their-predictions/2011867.article

Tucker B., (2012). The Flipped Classroom: Online Instruction at Home Frees Class Time for Learning. Education Next. 82–83. http://educationnext.org/the-flipped-classroom/

Tweney D., (2014). This French tech school has no teachers, no books, no tuition — and it could change everything. Venture Beat. http://venturebeat.com/2014/06/13/this-french-tech-school-has-no-teachers-no-books-no-tuition-and-it-could-change-everything/

United Nations Department of Social and Economic Affairs. (2014). World's Population Increasingly Urban With More Than Half Living in Urban Areas. www.un.org/en/development/desa/news/population/world-urbanization-prospects-2014.html

United Nations Population Fund. (2013). World Population Prospects. New York: United Nations. http://esa.un.org/wpp/documentation/pdf/wpp2012_highlights.pdf

United States Department of Education. Competency-Based Learning or Personalized Learning. http://www.ed.gov/oii-news/competency-based-learning-or-personalized-learning

World Bank. (2011). Multipolarity: The New Global Economy. Washington: World Bank, 2011. http://econ.worldbank.org/external/default/main?pagePK=64165259&theSitePK=469372&piPK=64165421&menuPK=64166322&entityID=000333037_20110620010206

World Health Organization: Global Health Observatory. (2014). Urban population growth, 2014. www.who.int/gho/urban_health/situation_trends/urban_population_growth_text/en/

Yonazi E., T. Kelly, N. Halewood, C. Blackman (eds). (2012). The Transformational Use of Information and Communication Technologies in Africa. Washington, DC: World Bank. http://web.worldbank.org/WBSITE/EXTERNAL/TOPICS/EXTINFORMATIONANDCOMMUNICATIONANDTECHNOLOGIES/0,,contentMDK:23262578~pagePK:210058~piPK:210062~theSitePK:282823,00.html

Zappa M., (2014). Envisioning the Future of Education Technology. http://www.envisioning.io/education/