Volume 1, Issue 3
March 2015

HDIAC Journal

The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC)

LINKS TO SPECIAL POINTS OF INTEREST:

Weapons of Mass Destruction

CBRN Defense

Biometrics

Alternative Energy

Technical Inquiry Highlight

Coming up next issue...

Calendar

Noteworthy

Biometric eye scanners, such as the one seen in this Feb. 27, 2011 photo, are used to process patients arriving at Bagram Airfield's Korean hospital in Parwan province, Afghanistan, Feb. 27, 2011. (U.S. Army photo by Sgt. Chris Hargreaves/Released)

HDIAC Journal

Volume 1, Issue 3

TABLE OF CONTENTS

WEAPONS OF MASS DESTRUCTION: ***Countering WMD (CWMD) Threats—Critical Step in Emergency Preparedness Against WMD*** **D. Metz**	3
CBRN DEFENSE: ***U.S. Homeland CBRN Emergency Preparedness Enterprise—a Retrospective Review*** **D. Metz**	7
BIOMETRICS: ***Applications of Biometrics for Immigration Management and Enforcement*** **C. Daub**	11
ALTERNATIVE ENERGY: ***The Electric Microgrid— An Economically-Viable Architecture for Energy Surety and Renewable Integration*** **C. Doran**	15
Technical Inquiry Highlight	22
Coming up next issue...	23
Calendar of Events	25
Noteworthy	26

About This Publication: The Journal of the Homeland Defense and Security Information Analysis Center (HDIAC) is published quarterly by the HDIAC staff. The HDIAC is a DoD sponsored Information Analysis Center (IAC) with policy oversight provided by the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), and it is administratively managed by the Defense Technical Information Center (DTIC). The HDIAC is operated by Information International Associates (IIA) in Oak Ridge, TN.

Countering WMD (CWMD) Threats—Critical Step in Emergency Preparedness Against WMD

D. Metz

In order to minimize or circumvent the effects of weapons of mass destruction (WMD), as related to the loss of life and property, emergency preparedness against WMD becomes an important countermeasure. Countering WMD is a critical element of the emergency preparedness process because it contains elements of prevention, mitigation and response.

Troops stand guard around a suspected "chemical weapons" facility during a training exercise at Fort Irwin's National Training Center. (DoD Photo by Guy Volb/Released)

This article will highlight some of the important ongoing efforts being conducted by the Department of Defense (DoD) and Department of Energy (DOE) to counter the threats posed by WMD and how those efforts apply to emergency preparedness. First, a brief discussion on some important U.S. documents that include the requirements for ensuring the security interests of the United States by countering WMD is provided.

On December 11, 2002, then President George W. Bush issued the *National Strategy to Combat Weapons of Mass Destruction*. In this strategy, President Bush stated that WMD, nuclear, biological and chemical, in the possession of hostile states and terrorists, represent one of the greatest security challenges facing the United States. The President further stated that our national strategy to combat WMD is based on three pillars: (1) counterproliferation, (2) nonproliferation and (3) consequence management. Those three pillars to combat (counter) WMD (CWMD) remain in effect today.

On May 27, 2010, President Obama issued the U.S. *National Security Strategy*. This strategy stated that there is no greater threat to the American people than WMD, particularly the danger posed by the pursuit of nuclear weapons by violent extremists and their proliferation to additional states. The President also stated that we are pursuing new strategies to protect against biological attacks, and he specifically called for "obtaining timely and accurate insight on current and emerging risks."

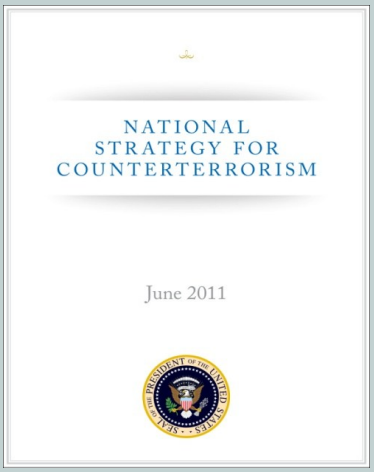
Soldiers with the New Hampshire and Massachusetts National Guard CBRNE enhanced response force packages (CERF-P) work to decontaminate personnel that have been evacuated or extricated out of a simulated collapsed structure. (Maine Army National Guard photo by Sgt. Angela Parady/Released)

Troops transfer a sample of simulated nuclear fallout during an exercise that helped test the Defense Department's chemical, biological, radiological, and nuclear enterprise, July 28, 2012. (U.S. Army photo by Lt. Col. Carol McClelland/Released)

Countering WMD (CWMD) Threats—continued

D. Metz

On June 28, 2011, President Barack Obama issued the *National Strategy for Counter-terrorism*. In this strategy, President Obama stated that nuclear terrorism is the greatest threat to global security. The President further stated that preventing terrorist development, acquisition and use of WMD is one of the eight overarching counterterrorism (CT) desired end states (goals) to achieve success in the U.S. global CT mission.

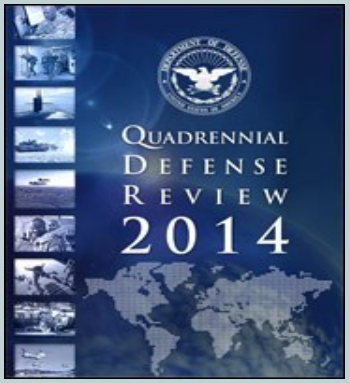


Cover of the National Strategy for Counterrorism (Courtesy of The White House/Released)

On January 5, 2012, the U.S. Defense Strategic Guidance (i.e., *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*) was released by then Secretary of Defense Leon Panetta. He stated that this guidance will "preserve our ability to conduct the missions we judge most important to protecting core national interests." One of those six missions is countering WMD.

On March 4, 2014, Secretary of Defense Chuck Hagel released the 2014 Quadrennial Defense Review (QDR). The QDR is a legislatively-mandated review of Department of Defense (DoD) strategy and priorities. The QDR describes how our military will prepare for the strategic challenges and opportunities that will be faced in the future (typically, the next 10 years) framed within the current constraint of fiscal austerity.

One section of the QDR contains an assessment of the QDR by General Martin E. Dempsey, Chairman of the Joint Chiefs of Staff. He states that he and the Joint Chiefs used the prioritization of 12 identified missions to advise the Secretary of Defense and the President and determine how to distribute the force among our Combatant Commanders. CWMD is the sixth most important mission of the 12 identified missions.



Cover of the 2014 Quadrennial Defense Review (Courtesy of DoD/Released)

Information was provided on April 1, 2014 by (1) Ms. Rebecca K. C. Hersman, Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction; (2) Ms. Anne Harrington, Deputy Administrator for Defense Nuclear Proliferation Office, National Nuclear Security Administration (NNSA), DOE; and (3) Mr. Kenneth A. Myers III, Director of Defense Threat Reduction Agency (DTRA) and Director of U.S. Strategic Command Center for Combating Weapons of Mass Destruction (SCC-WMD), during the hearing entitled "Proliferation Prevention Programs at the Department of Energy and Department of Defense." This hearing was held before the Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee. The overarching focus of the hearing was framed within the Fiscal Year (FY) 2015 President's budget request for these organizations. Three expert witnesses provided the details of the ongoing CWMD efforts, and their testimony is presented in the following paragraphs.

Ms. Harrington stated that one of the most important missions of her organization has been to support the Administration's commitment to secure the most vulnerable nuclear material across the globe, commonly referred to as the four year effort. In particular, NNSA accomplishments since 2009 have included the following: removed or confirmed the disposition of about 3,000 kilograms of highly enriched uranium (HEU) and separated plutonium including the removal of all HEU from 11 countries and Taiwan; enhanced security of 32 buildings containing metric tons of weapon-usable material in Russia; installation of almost 1,600 radiation portal monitors at border crossings, airports and seaports; and successful removal of quantities of HEU from both Italy and Belgium.

Countering WMD (CWMD) Threats—continued

D. Metz

Ms. Anne Harrington, Deputy Administrator for Defense Nuclear Proliferation Office, National Nuclear Security Administration (NNSA), DOE, at the "Proliferation Prevention Programs at the Department of Energy and Department of Defense" hearing held before the Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee. (Courtesy of The U.S. Senate/Released)

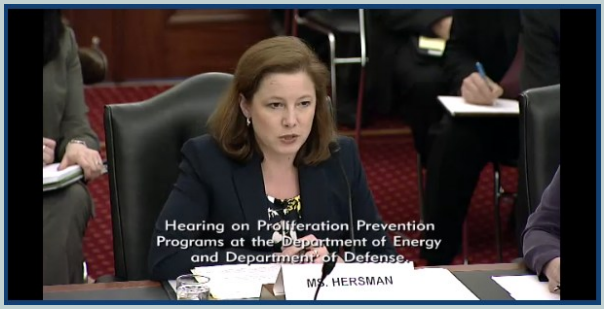
She noted that the highlight at the third Nuclear Security Summit in the Hague in late March 2014 was the joint U.S.-Japan announcement to eliminate hundreds of kilograms of HEU and plutonium from the Japanese Atomic Energy Agency's Fast Critical Assembly. She stated that these accomplishments have made it substantially more difficult to acquire and traffic the materials required to make an improvised nuclear device.

"Countering such complex and dynamic threats of WMD requires flexible, innovative and agile response…"

She also mentioned that with support from Congress her office will continue to pursue a multi-layered approach to protect and account for materials at their source; remove, down-blend or eliminate material when possible; detect, deter and reduce the risk of additional states acquiring nuclear weapons; support the development of new technologies to detect nuclear trafficking and proliferation; and verify compliance with arms control treaties.

Ms. Hersman stated that countering such complex and dynamic threats of WMD requires flexible, innovative and agile responses as well as "whole-of-department," "whole-of-government" and even "whole-of-international-community" solutions. She noted that the international efforts to deal with Syria's chemical weapons (CW) program, which is unprecedented in scale, speed and complexity, is a vivid example. She went on to state that because of the efforts of so many contributors and the support of Congress, Syria's CW program is on the path to elimination. The centerpiece of the U.S. contribution, the Cape Ray (a former U.S. cargo ship), outfitted with DoD's recently-developed Field Deployable Hydrolysis Systems and funded predominantly through the Cooperative Threat Reduction (CTR) program, is ready to neutralize the most dangerous chemicals in the Syrian arsenal and to do so in a safe, secure and environmentally sound fashion. She emphasized that this type of creative, collaborative approach to a WMD challenge cannot be the exception but must become the rule.

Another case in point cited by Ms. Hersman is the January 2014 announcement of the complete destruction of the CW munitions that Libya declared in 2011 and 2012. She cited this success as possible only through the resources and expertise coupled with cooperation from the OPCW and Libyan government with contributions from the German government.



Ms. Rebecca K. C. Hersman, Deputy Assistant Secretary of Defense for Countering Weapons of Mass Destruction, at the "Proliferation Prevention Programs at the Department of Energy and Department of Defense" hearing held before the Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee. (Courtesy of The U.S. Senate/Released)

She stated that even though the traditional DoD CTR Program of assistance that has operated in Russia for the last 20 years is drawing to a close, the United States and Russia have agreed to continue a number of important efforts on a collaborative basis through the Framework Agreement and Protocol on a Multilateral Nuclear Environmental Programme in the Russian Federation (MNEPR), of which NNSA is a partner. She mentioned that Russia and the United States plan to proceed through the DoD CTR program with two already planned projects: dismantling a Delta III strategic submarine and funding transportation of HEU submarine spent fuel from a less secure to a much more secure location in Russia. She believed these efforts to be priority threat reduction activities important to the U.S. national security interest. She did state that given the unfolding events in Ukraine and Crimea, her office is carefully evaluating their activities in the region to ensure full consistency with the President's guidance.

Countering WMD (CWMD) Threats—continued

D. Metz

Ms. Hersman also discussed efforts being undertaken by her office regarding the biological threat. She mentioned the Cooperative Biological Engagement Program (CBEP), which is part of the DoD CTR program, includes active engagements in Africa, South and Southeast Asia, and the Middle East to address the diverse and rapidly changing global biological threat.

She also stated that the CBEP attempts to reduce biological threats by focusing on security, enhanced security measures and securing pathogens as well as improving our ability to survey, detect and provide better strategic warnings for biological threats. She indicated that the CBEP collaborates very closely with its many partners, including the State Department and the expertise resident in the Centers for Disease Control and Prevention (CDC).

Mr. Kenneth A. Myers III, Director of Defense Threat Reduction Agency (DTRA) and Director of U.S. Strategic Command Center for Combating Weapons of Mass Destruction (SCC-WMD) at the "Proliferation Prevention Programs at the Department of Energy and Department of Defense" hearing held before the Subcommittee on Emerging Threats and Capabilities of the Senate Armed Services Committee. (Courtesy of The U.S. Senate/Released)

Mr. Myers discussed the work being done by DTRA and SCC-WMD to counter the threats posed by the proliferation and use of WMD. He highlighted three of their recent activities.

He stated that one of the best examples of the capabilities that DTRA/SCC-WMD can provide and the missions they take on is related to their work in Syria. He noted that they had the expertise to evaluate a serious threat, developed the needed technologies and provided planning support to all aspects of the operation. Now the Cape Ray stands ready to begin destruction once all the chemical materials are out of Syria.

Another critical area for DTRA/SCC-WMD is the intersection of terrorism and acquisition of WMD materials, particularly biological threats. He stated this is an emerging and evolving threat, and they are expanding their areas of cooperation to stay one step ahead.

He emphasized that DTRA/SCC-WMD work closely with the CDC, and that they often pursue global health security projects together, internationally. He noted that the CDC handles public health issues, but they are not equipped to address the security threats posed by deadly pathogens, whereas DTRA/SCC-WMD is. He mentioned that earlier this year, DTRA/SCC-WMD signed a memorandum of understanding (MOU) and a strategy for joint work with CDC. This collaboration will maximize their effectiveness related to biological threats around the world. He also mentioned that DTRA/SCC-WMD recently completed the destruction of weaponized mustard agent in Libya. He cited that 517 mustard filled artillery rounds, eight 500-pound aerial bombs and 45 insert tubes were destroyed.

The Benjamin Franklin axiom that "an ounce of prevention is worth a pound of cure" is as true today as it was when Franklin made the quote in 1735. This axiom is especially relevant to DoD efforts focused on CWMD. The efforts being undertaken by DoD and DOE in the WMD proliferation prevention arena are critical to establishing emergency preparedness against WMD. Their continued collaborative efforts in CWMD should yield an effective "ounce of prevention."

About the Author:

Mr. Dennis Metz, Vice President of SciTech Services, Inc., has over 41 years of experience in chemical and biological warfare, chemical and biological defense, target defeat, and WMD casualty effects technology areas. Mr. Metz has conducted projects encompassing all chemical and biological defense functional areas, ranging from threat modeling, detection, decontamination and protection to arms control.

U.S. Homeland CBRN Emergency Preparedness Enterprise—a Retrospective Review

D. Metz

Much can be learned from past history. Therefore, this article will study the elements comprising the U.S. Homeland CBRN emergency preparedness enterprise of 1962 versus 2014 and address their similarities and differences. In 1962, the Cuban Missile Crisis occurred over a 13 day period in October. The crisis centered on the former Soviet Union placing intermediate-range nuclear missiles in Cuba.

U.S. Navy low-level photograph of San Cristobal MRBM site no. 1on October 23, 1962. (Courtesy of "The Cuban Missile Crisis, 1962: The Photographs," Dino A. Brugioni Collection, The National Security Archive, The George Washington University/Released)

The Cuban Missile Crisis was the closest the world ever came to a nuclear war. Fortunately, the negotiating efforts of President John F. Kennedy and Premier Nikita Khrushchev averted a nuclear war.

In 1961, President Kennedy created the Office of Emergency Preparedness inside the White House to handle the growing risk of natural disasters. He also created the Office of Civil Defense (OCD) in July 1961, which was part of the Department of Defense (DoD). As specified in the Presidential Executive Order 10952 dated July 20, 1961, the OCD was charged with, among several other duties, the "…development and execution of (i) a fallout shelter program; (ii) a chemical, biological and radiological warfare defense program; and (iii) all steps necessary to warn or alert Federal military and civilian authorities, state officials and the civilian population."

1962 Civil Defense Bus/Subway Poster (Courtesy of www.civildefensemuseaum.com/Released)

President Kennedy advocated the use of fallout shelters as part of the U.S. response to survive a nuclear attack by the Soviet Union. He believed the lives of families not directly hit in a nuclear attack could be saved if they could take shelter.

On August 14, 1961, President Kennedy signed Executive Order 10958. It delegated responsibility for civil defense food stockpiles to the Secretary of Agriculture and also civil defense medical stockpiles to the Secretary of Health, Education and Welfare (HEW).

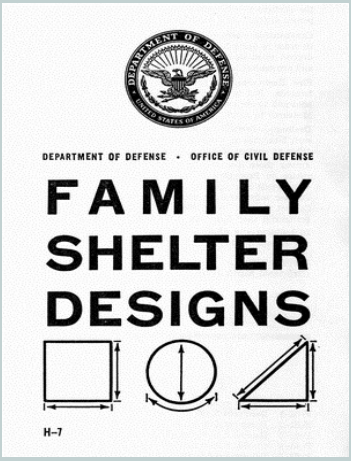
Civil Defense Light-Up Display Transparency (Courtesy of www.civildefensemuseaum.com/ Released)

In the summer of 1961, at the request of President Kennedy, Congress appropriated $207.6 million to identify and mark spaces in existing buildings for fallout shelters, stock the shelters with food and other supplies, improve air-raid warning systems and include space for shelters in new Federal buildings. With these funds, the OCD, assisted by the Army Corps of Engineers and the U.S. Navy's Bureau of Yards and Docks, began organizing surveys to identify possible fallout shelter spaces for 104 million Americans in existing structures. The OCD also began distributing large numbers of "Shelter Radiation Kits" that contained survey meters and dosimeters to public shelters and monitoring stations. OCD enacted many

U.S. Homeland CBRN Emergency Preparedness Enterprise—continued

D. Metz

programs against the threat of a Soviet nuclear attack. This included booklets, brochures and videos on ways to protect one's self and how to build a backyard or basement bomb shelter.



H-7 Family Shelter Designs handbook published in January 1962 by the Office of Civil Defense. (Courtesy of DoD/Released)

On February 16, 1962, Presidential Executive Orders 10997 through 11005 assigned emergency preparedness functions to the Secretary of the Interior, Secretary of Agriculture, Secretary of Commerce, Secretary of Labor, Secretary of HEW, Postmaster General, Administrator of the Federal Aviation Agency, Housing and Home Finance Administrator, and the Interstate Commerce Commission. Each one was required to prepare national emergency plans and develop preparedness programs. These plans and programs were designed to develop a state of readiness in these areas with respect to all conditions of national emergency, including attack upon the United States. The "attack upon the United States" included chemical, biological and radiological (CBR) attacks.

The focus of the U.S. civil defense program in the early 1960s was predominantly concerned with a nuclear strike by the Soviet Union against our homeland. The fallout shelters that were constructed during this period were designed to protect against nuclear fallout and not against chemical and biological agents.

On June 19, 1978, President Carter established the Federal Emergency Management Agency (FEMA). The role of FEMA was to consolidate emergency preparedness, mitigation and response activities into one federal emergency management organization. Until 2001, the U.S. civil defense duties were performed by FEMA. After the September 11, 2001 terrorist attacks against the United States, President George W. Bush issued Executive Order 13228 on October 8, 2001, establishing the Office of Homeland Security (OHS) and the Homeland Security Council.

The north face of Two World Trade (south tower) immediately after being struck by United Airlines Flight 175 on September 11, 2001. (Courtesy of Wikimedia Commons/Released)

The function of the OHS was to coordinate the executive branch's efforts to detect, prepare for, prevent, protect against, respond to and recover from terrorist attacks within the United States. OHS became the Department of Homeland Security (DHS) on November 25, 2002 by the Homeland Security Act of 2002. The five core missions of DHS are the following: (1) prevent terrorism and enhance security, (2) secure and manage our borders, (3) enforce and administer our immigration laws, (4) safeguard and secure cyberspace, and (5) ensure resilience to disasters.

FEMA was absorbed into DHS effective March 1, 2003. As a result, FEMA became part of the Emergency Preparedness and Response Directorate of DHS. It became FEMA again on March 31, 2007 but remains in DHS. FEMA has the U.S. civil defense mission as it relates to the U.S. national preparedness mission.

In January 2012, a new strategic guidance, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense*, was developed for DoD for sustaining U.S. global leadership for a 21st century defense. This guidance reflected President Obama's strategic direction to DoD. Primary missions of the U.S. Armed Forces specified in this strategic guidance included counter terrorism, defend the homeland, provide support to civil authorities, and counter weapons of mass destruction (WMD).

U.S. Homeland CBRN Emergency Preparedness Enterprise—continued

D. Metz

As specified in Joint Publication 3-27, *Homeland Defense*, dated July 29, 2013, DoD is responsible for the homeland defense (HD) mission against employment of CBRN weapons directly against the United States. DoD leads the response with support from international partners and U.S. Government (USG) departments and agencies. DHS is the lead federal agency for homeland security (HS). DoD supports HS against possible covert CBRN weapons.

The 2014 Quadrennial Defense Review (QDR) was released by the Secretary of Defense on March 4, 2014. The QDR is a legislatively-mandated review of DoD strategy and priorities. The 2014 QDR prioritizes three strategic pillars in a period of fiscal austerity: (1) defend the homeland, (2) build security globally, and (3) project power and win decisively. The QDR discusses a world that is growing more volatile, more unpredictable, and in some instances, more threatening to the United States.

One section of the QDR contains an assessment of the QDR by General Martin E. Dempsey, Chairman of the Joint Chiefs of Staff. He states that he believes there are six national security interests for which we are responsible [Note: These are directly derived from the four core interests outlined in the National Security Strategy]. The first two are: (1) survival of the nation and (2) prevention of catastrophic attack against U.S. territory. He goes on to state that based on these six interests, he and the Joint Chiefs used the prioritization of 12 identified missions to advise the Secretary of Defense and President and determine how to distribute the force among our Combatant Commanders. The first and second most important missions are the following: maintain a secure and effective nuclear deterrent and provide for military defense of the homeland. The fifth and sixth most important missions are combat terrorism and counter WMD.

"The 2014 QDR prioritizes three strategic pillars… defend the homeland, build security globally, and project power and win decisively."

Funding for homeland defense against CBRN weapons remains a high priority. In the FY 2014 omnibus appropriations bill signed into law on January 17, 2014, DHS funding for such purpose includes the following:

- $81 million to implement "standards" to prevent terrorists from gaining access to chemicals that can be converted into WMDs
- $85 million for the BioWatch program to improve the Nation's biological detection capabilities
- $404 million for the National Bio and Agro Defense Facility to conduct research to prevent the accidental or intentional introduction of deadly animal diseases into the U.S.
- $285 million for the Domestic Nuclear Detection Office to improve the Nation's capability to detect and report unauthorized attempts to import, possess, store, develop or transport nuclear or radiological material for use against the Nation

Soldiers from the Maryland Army National Guard's 231st Chemical Company, based in Greenbelt, Md. scan a simulated village for chemical weapons during a Sept. 8, 2013 training exercise at Gunpowder Military Reservation. (National Guard photo by 1st Lt. Kristofer Baumgartner/ Released)

U.S. Homeland CBRN Emergency Preparedness Enterprise—continued

D. Metz

When one compares the elements of CBRN emergency preparedness in 1962 versus 2014, the similarities are the following:

- Protection of the homeland to deter and defeat attacks on the United States is of the highest importance.
- DoD leads the homeland defense mission, if the homeland is attacked by CBRN weapons.
- Our nuclear deterrent is the ultimate protection against a nuclear attack on the United States.
- Guidance/direction on protection of the homeland has emanated from the President of the U.S.
- The Homeland CBRN emergency preparedness enterprise entails both non-DoD and DoD entities and requires coordinated and integrated activities among and between these different organizations.
- Homeland defense against CBR (CBRN) attacks is a very high priority.

Several differences that exist today versus 1962 are the following:

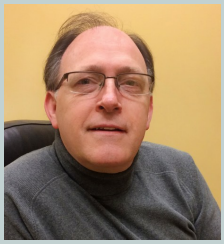
- U.S. Homeland CBR civil defense (emergency preparedness) mission resided with DoD in 1962, and today the CBRN emergency preparedness mission is with FEMA in DHS.
- In 1962, the nuclear capable nations, for all intents and purposes, were the U.S. and the Soviet Union. Today, the number of nuclear capable nations is much larger and continues to grow.
- Today, terrorist networks continue to demonstrate interest in obtaining WMD. Terrorist attacks involving WMD were not really considered a threat in 1962.

The CBRN threats today are more diverse and broader than the ones in 1962. The CBR emergency preparedness enterprise of 1962 had many elements in common with the CBRN emergency preparedness enterprise of today. However, the key difference between the CBRN emergency preparedness enterprise of today versus 1962 is that the full spectrum of CBRN threats drives the enterprise; whereas in 1962, the nuclear threat was the predominant threat driving the enterprise.

"Homeland defense against CBRN attacks is a very high priority."

About the Author:

Mr. Dennis Metz, Vice President of SciTech Services, Inc., has over 41 years of experience in chemical and biological warfare, chemical and biological defense, target defeat, and WMD casualty effects technology areas. Mr. Metz has conducted projects encompassing all chemical and biological defense functional areas, ranging from threat modeling, detection, decontamination and protection, to arms control.



Applications of Biometrics for Immigration Management and Enforcement

C. Daub

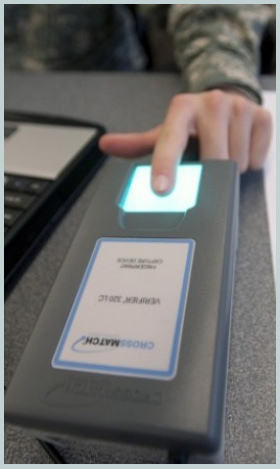
Immigration control remains a challenge for the United States and many other nations around the world. While some of the leading immigration issues vary according to the times, other issues are perennial until a suitable solution is found. Knowing exactly *who* is being granted entry to a nation is one of the preeminent problems today, and it has become vastly more important with the global spread of extremism and terrorism. Some of the tools used to mitigate this problem have changed very little over the centuries (e.g., walls, fences, passports and border guards), but as technology progresses, we have found new means to enforce laws and to make existing precautions more potent. Biometrics has become the most powerful, and perhaps most discussed, implement of the last few decades to better organize and strengthen immigration control. This article will explore current and proposed biometric collection programs, state-of-the-art modalities, devices that might be leveraged, and possible advantages and obstacles that must be overcome to create a balanced and reliable immigration system for the future.

Although biometrics is a modern term, elements of what we consider to be biometrics have been in use for far longer in the quest for a robust immigration control system. What is often called "facial recognition" today has been in use since the beginning of human civilization and is used by almost everyone on a daily basis to recognize friends, acquaintances and enemies. By extension, photography, since its invention, has provided a means of storing a person's facial image in travel documents, ID cards and criminal databases for future authentication. The newest frontier in facial recognition is the use of automated systems to identify persons from stored imagery data to streamline identification procedures.

"What is often called 'facial recognition' today has been in use since the beginning of human civilization…"

While still several years off, there appears to be the promise of using automated systems to correctly identify a person without the need for close scrutiny from a customs official, which should greatly lower wait times at border crossings or ports of entry. Facial recognition using sophisticated computers and software is still very much an imperfect science. Almost any individual can compare a photograph to a person's face with some degree of accuracy, but computers often have difficulty unless the images are captured under very favorable conditions. While it is a difficult task to covertly perform facial recognition in busy environments, such as airports, overt collection will continue to improve because of the standardization and control of the immediate collection environment. High-resolution cameras are needed to provide images with enough quality to aid in identification. For covert collection, movement of a subject can interfere with the image quality; therefore, the systems need to be able to take motion stills and have algorithms to recognize subjects at angles other than head-on. Furthermore, facial recognition is the most easily fooled, or "spoofed," means of identification. Obstructions, such as facial hair, eyeglasses and headwear, can prevent the recognition of the full facial structure of a person, hence the great advantage of overt collection done with the assistance of a collector and participant. Despite its current shortcomings, automated facial recognition, both overt and covert, will only become a more effective central technology in the future of immigration biometric systems.

To a lesser extent than facial recognition, fingerprint capturing has also been a useful tool in immigration control for several decades. Combined with a photograph of a person's face, the inclusion of a fingerprint on passports or other documents has long been recognized as an effective means for accurately verifying identity. Fingerprinting became understood and utilized as a unique identifier in the late 19th century, and the method of capture has progressed from ink prints to the use of live-scan technology to improve the speed and convenience of collecting data. As a means of recognition, fingerprinting is both accurate and reliable and works best when used in conjunction with other modalities, such as facial recognition or iris scans. Many passports and identification cards that are issued today include a fingerprint scan imbedded in a chip to provide a record for comparison when an individual's fingerprints are captured using live-scan systems.



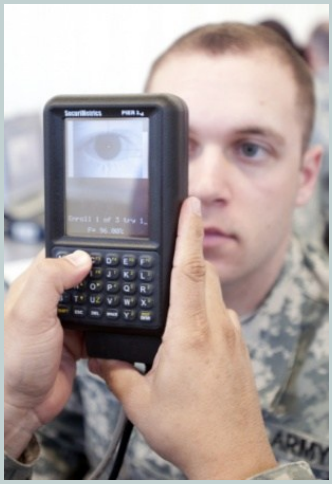
Soldiers learn how to use the Crossmatch 300, a fingerprint scanning device that is part of the biometrics automated tool-set. (U.S. Army photo by Staff Sgt. Lewis Hillburn/Released)

Applications of Biometrics for Immigration Management—continued

C. Daub

Iris scanning was developed as an identification technology in the 1990s and rapidly expanded in the post-9/11 era to become a sort of gold standard as a biometrics modality. The human iris has extremely complex and delicate patterns that are readily visible and change very little, if at all, during a person's life. The development of algorithms to chart and record these patterns and readily interpret them to identify an individual has progressed to the level that these systems are extremely fast, efficient and accurate.

Despite these advantages, iris scanners are generally more costly than older forms of biometrics systems, such as fingerprinting, and they require the subject to be within a few meters of the scanning machine. Owing to the great advantages of iris recognition, systems are being widely tested and installed at ports of entry, especially airports, to provide speedy and extremely accurate identification.



Pfc. Jason McCune sits while his iris is scanned during a biometrics class. (U.S. Army photo by Staff Sgt. Lewis Hillburn/ Released)

Dozens of countries around the world have already embraced biometric passports as a fundamental element of improved security. These passports use contactless smart card technology by embedding a microprocessor chip somewhere within the passport booklet that stores fingerprint, facial and/or iris data, depending on the standards adopted by the issuing nation. Among countries using biometric passports are the United States, all nations in the European Union, Russia, Australia, Brazil, Argentina, the People's Republic of China and many others. Some nations, such as India, have announced the intention of providing biometric passports to its citizens. In the United States, the US-VISIT program was developed to collect biometric data, particularly photographs and 10-print fingerprint scans, from individuals visiting the country to check the data against a database of illegal immigrants, terrorists and criminals. Individuals who are watch-listed as possibly being a risk can be tracked and recognized at ports. This responsibility is now handled by the Office of Biometric Identity Management (OBIM). Similar programs were adopted by other nations such as Japan (J-VIS) and South Korea (ROK-VISIT) to manage access to their borders as well.

Development continues to build on the successes of current programs, mitigating limitations and streamlining processes to efficiently handle the volume of visitors encountered at ports of entry without sacrificing accuracy. The Department of Homeland Security (DHS) has established a testing facility to replicate real-world conditions in order to assess the effectiveness of iris scanning and facial recognition systems and how to best deploy the systems to track entries and departures from the country through major airports. This effort is not only to improve screening times and accuracy but also to electronically track individuals to ensure that they have left the country when their visas expire. [1]

A person using the US-VISIT scanner at a customs check point. (Courtesy of Wikipedia/Released)

Addressing the drawbacks of the current technologies in use is one of the most important parts of the equation. Research is ongoing to lessen or eliminate the disadvantages of certain systems and to offer greater functionality in challenging environments. For instance, the DoD has invested in research projects, such as one at Carnegie-Mellon University that is attempting to create a single system that can perform both facial recognition and iris scanning simultaneously at distances of up to 12 meters. Benefits would include faster processing of people in queues and greater stand-off for security personnel who might have to confront dangerous subjects attempting to enter the country. [2]

Applications of Biometrics for Immigration Management—continued

C. Daub

U.S. Customs is also preparing to introduce biometric technology to secure border crossings with Mexico, specifically using facial recognition systems to track individuals exiting the country. This type of application of automated biometric systems will be a particular challenge owing to the conditions often encountered at border crossings: moving traffic, obstructions such as windscreens and window tinting, and long lines. Development of a robust system that can accomplish these tasks reliably in adverse conditions would be a further benefit for applications in other challenging environments. [3]

Lines of cars waiting at the Mexico/United States border crossing. (Courtesy of Reuters/Released)

Elsewhere, Australia has begun implementing e-Gate systems in its major airports to track individuals entering and exiting the country. The need for increased security came into focus in June 2014 when reports of possible issues in the Australian immigration tracking system allowed a convicted terrorist to leave the country. The e-Gate systems use biographic data such as name, address and birthdate coupled with a live-scan fingerprint capture to track an individual. Eventually, Australian Customs intends to apply facial recognition technology along with the e-Gates to further fortify their biometrics tracking efforts. [4]

"U.S. Customs is also preparing to introduce biometric technology to secure border crossings with Mexico, specifically using facial recognition systems to track individuals…"

Photo of the e-GATE system at the London Heathrow Airport in Terminal 4. (Courtesy of Wikipedia/Released)

Malaysia's immigration department is also planning to introduce a comprehensive biometric system to aid in managing ingress and egress of visitors. Malaysia planned on introducing this system by the end of 2014, with specific aims at limiting drug smuggling, human trafficking, freedom of movement for terrorists, and to possibly help with unforeseen crises such as Malaysian Air Lines flight MH370, which went missing 8 March 2014 under suspicious circumstances. Iris scanning and facial recognition technology will be employed to identify passengers and visitors at airports to complement existing procedures and abolish loopholes. These updates will also be accompanied by other security precautions, such as integrating records with Interpol databases for stolen or lost travel documents, improved passport scanning systems, high definition closed-circuit security camera and television systems, and improved passenger screening. [5]

While the tools to enforce immigration law are becoming more powerful, policy and training must be capable of following suit to ensure that any gaps in the system are addressed. For instance, in the United States, multiple federal agencies such as the DHS, DoD and Department of State (DoS), as well as many of their sub-agencies, have biometric data responsibilities. The necessity of information sharing across these agencies is of paramount importance to assure that not only are all machines and captured data standardized and up-to-date, but that any needed data is also easily accessible for immigration officials. It would be unconscionable if an identified terrorist from a nation, such as Iraq, were granted access into the United States, particularly if this individual's biometric data was previously cataloged and watch-listed by DoD collection efforts in that nation. Any break in the chain of sharing of data or watch-lists could result in a breach of security and could possibly jeopardize lives.

Applications of Biometrics for Immigration Management—continued

C. Daub

Policy must also keep pace with developments in immigration. Policy improvement or implementation commonly trails behind events that shed light on some sort of deficiency. Biometric systems, when properly employed, provide a reliable means of identifying individuals who might have illegal intentions, but knowing what to do with those individuals can be just as important. If an individual is caught attempting to enter the United States illegally, are there proper regulations in place that give clear direction on how they should be handled? The answer is sometimes no. For instance, in spring of 2014, children from Central America who illegally entered the United States to unite with parents who had also illegally entered and stayed in the United States were sent to live with those parents rather than being deported. Although the law allows for the children to remain in the United States to protect them rather than deporting them as adults would be, this apparent contradiction caused Judge Andrew S. Haden to state, "The DHS is rewarding criminal conduct instead of enforcing the current laws. More troubling, the DHS is encouraging parents to seriously jeopardize the safety of their children." [6]

"Policy must also keep pace with developments in immigration."

Lastly, training must also be sufficiently available and implemented to avoid costly mistakes. The best automated biometric systems, progressive strategies and policies put in place can be meaningless if those responsible fail to use the systems in the proper manner or apply appropriate policy accordingly. While biometric systems are becoming more complex and automated, training will need to become more intense and well rounded to guarantee that the data collected is accurate and shared in a timely and efficient manner following the procedures set in place.

Though challenges with immigration systems and enforcement will always remain and change with the times, biometric systems will continue to evolve to help mitigate and anticipate many of the difficulties. Once established, identity dominance in the field of immigration will allow for even greater accuracy of recognition, documentation and enforcement of the law. These efforts will offer the greatest amount of protection to citizens, while ensuring that immigrants and visitors are treated fairly.

U.S. Soldiers of Headquarters Company, 2nd Battalion, 8th Cavalry Regiment, 1st Brigade Combat Team, 1st Cavalry Division use the Biometrics Automated Tool Set system. (Courtesy of DoD/Released)

References:

[1] http://goo.gl/IJSytY
[2] http://goo.gl/JpEVVj
[3] http://goo.gl/1Hdr3K
[4] http://goo.gl/y8Ec2g
[5] http://goo.gl/U9gljH
[6] http://goo.gl/3VmrFU

About the Author:

Mr. Christopher Daub is a biometrics subject matter expert who worked for Northrop Grumman Corporation as a business development representative and analyst. He has seven years of military and private industry experience in military intelligence. Prior to his current position, Mr. Daub spent four years at the National Ground Intelligence Center in Charlottesville, VA as a drilling reservist and contracting subject matter expert on IEDs and biometrics analysis. He holds a B.A. in Political Science from Indiana University – Bloomington.

The Electric Microgrid— An Economically-Viable Architecture for Energy Surety and Renewable Integration

C. Doran

The U.S. electric infrastructure has essentially remained unchanged in its architecture for the past century. From an engineering perspective, this architecture has scaled remarkably well across the continent and has demonstrated impressive reliability, all things considered.

The classical centralized-generation grid architecture was designed toward the economies of scale and has achieved remarkably high effectiveness for that architectural paradigm. However, this architecture imposes efficiency and environmental ceilings because of the low penetration of renewable energy, lack of intelligent distribution, minimal (if any) storage, ad-hoc dispatch, uncontrolled load, and high distribution losses as power is moved large distances from generator to consumer. [1]

With a society increasingly reliant on electrical power, the once-good enough standard architecture based on centralized generation, arterial transmission and radial distribution is beginning to fall short for many critical applications. Microgrids offer a mechanism to intelligently compartmentalize the grid and provide additional focused measures for reliability where needed for absolutely critical loads, such as hospitals, data centers and military bases.

"A microgrid is a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid…"

While definitions vary slightly from source to source, the United States Department of Energy's definition of a microgrid puts it comprehensively and succinctly in the context of the broader electrical grid infrastructure. "A microgrid is a group of interconnected loads and distributed energy resources within clearly defined electrical boundaries that acts as a single controllable entity with respect to the grid; a microgrid can connect and disconnect from the grid to enable it to operate in either grid connected or islanded mode." [2]

The U.S. Army's RDECOM adds further specificity by stating that the microgrid is "capable to store, distribute, manage, import and export power, and interface with other relevant grids." In its typical implementation, the microgrid is independently managed and maintains only a single Point of Common Connection to the broader utility grid. This concept, espoused strongly by the Consortium for Electric Reliability Technology Solutions (CERTS) early on, ensures that the microgrid can be seen by the broader grid not as a collection of multiple diverse distributed generators and loads, but as a single entity; one that can appear as a load, an energy resource or nothing at all when operating in island mode. [3] In grid -connected mode, the microgrid can consume or provide electricity to the utility.

Example of a customer microgrid at Tohoky Fukushi University, Japan. (Courtesy of lbl.gov/Released)

The concerns associated with the ageing electrical infrastructure are not new to policy makers and system designers. The well-publicized Smart Grid initiatives strive to modernize the current "dumb grid" through high sensor density, improved communication networks, automated self-healing mechanisms and enhanced cyber security. In a fantastic symbiotic fashion, the Smart Grid and microgrids are able to provide significant mutual benefit. [4]

To the first degree, this is in the form of technology overlap, especially with respect to sensors, communications, power electronics and automated management systems. The second degree lies with the Smart Grid's Advanced Metering Infrastructure (AMI), which includes a two-way communication path between the utility and consumer for usage, pricing and sensing. This has the potential to dramatically open up the electricity market such that microgrids can become direct economic players and dispatchable resources to the utility to aid automated healing.

Because of the vast scale of the existing electricity grid (over a terawatt across hundreds of thousands of miles of power lines), [5] retrofitting to a full smart grid that is self-healing, secure and full of renewables is a daunting task for utilities, both in terms of technology and cost.

The Electric Microgrid— continued

C. Doran

However, by using a microgrid to integrate renewable generation resources in locally-managed fashion together with storage and inertial generation means that intermittency problems can be blunted before reaching the point of common connection to the grid. Because microgrids enable generation to be safely distributed across the grid, infrastructure upgrades along congested power arteries can be delayed. Thus, microgrids, which appear to the utility as self-contained loads/generators, much like the grid already has, are being perceived as handy ways to locally and modularly address needs to upgrade the grid, especially in the areas that need it most. [6]

"The grid is based on century-old technology and remains subject to the vulnerabilities inherent in its centralized architecture."

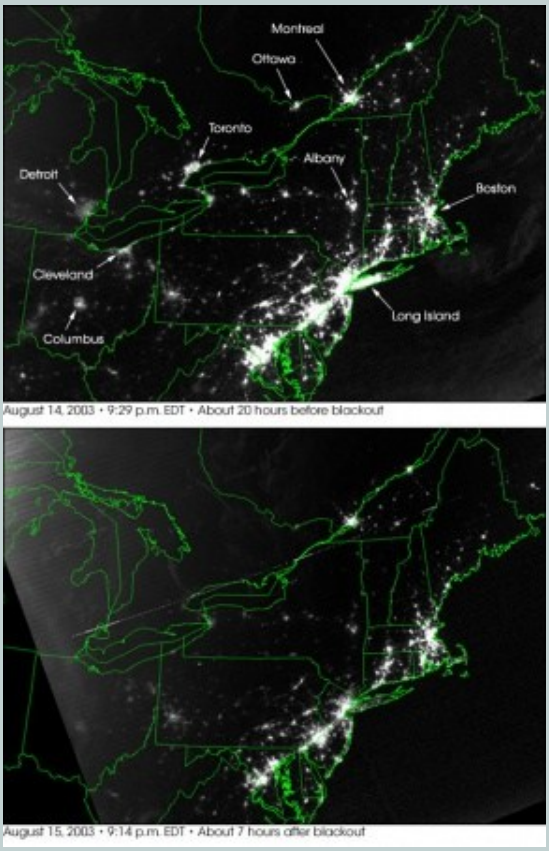
Energy surety

The United States' electric grid is among the most reliable in the world, yet there is a very good chance that you, the reader, have experienced a grid failure in the last 15 years. Move to a different country and that same cumulative likelihood of failure could exist over the past 15 days.

Guaranteeing the availability of electricity to critical loads is important enough that the buildings that house them are required to install their own backup generators and diesel tanks for times when the power goes out. These critical loads could include hospitals, emergency response centers, data centers, water pumping/filtration and operations centers for the military. The 2010 Quadrennial Defense Report defines energy security as "having assured access to reliable supplies of energy and the ability to protect and deliver sufficient energy to meet operational needs," and this is a requirement for the electricity supply (United States DoD, Quadrennial Defense Review Report (2010)).

The grid is based on century-old technology and remains subject to the vulnerabilities inherent in its centralized architecture. Instabilities could result from any variety of natural disaster, accident, strike or act of terrorism. The most troubling examples are the outages that cascade from grid segment to grid segment as generators become overloaded and disconnect to maintain safety. One might recall the massive blackout across the U.S. Northeast in August 2003, which removed light for over 50 million people within eight minutes as 261 power plants tripped off. It cost the economy an estimated $10 billion by conservative measures. [7]

One could also recall the more recent outage on the opposite corner of the continental U.S. in 2011, which was caused by a single human's operator error but cascaded across the southwest. Even in local-outage cases, the results of a power failure can be dangerous.



Before (top) and after (bottom) photos of a power failure that left many American cities in the dark on the evening of Thursday, Aug. 14, 2003. (Courtesy of NASA/Released)

For example, consider the heat wave of July 2006 when power to the FAA's Los Angeles Air Route Traffic Control Center covering parts of Arizona, Nevada, Utah and California shut down. It could not restore radar and communications for an hour and a half while it waited for a backup generator to activate, effectively incapacitating Los Angeles International Airport. [8]

Islandable microgrids offer a mechanism for sites to add self-sufficient managed capacity for backup generation to prioritized loads in the case of grid failure. At the same time, microgrids provide a higher level of stability back to the grid as a whole by compartmentalizing distributed generation and managed loads.

The Electric Microgrid— continued

C. Doran

In this scenario, a single generator failure is far less likely to cause a cascading failure across the entire grid; the microgrids can detect the instability and increase their output (or disconnect entirely), reducing the load on the remaining grid generators.

Microgrid technology is at least as important to the DoD as it is to any other customer. Some domestic bases experience power outages as often as 300 times per year, and forward-operating bases may need to operate without the luxury of any local grid support at all. [9]

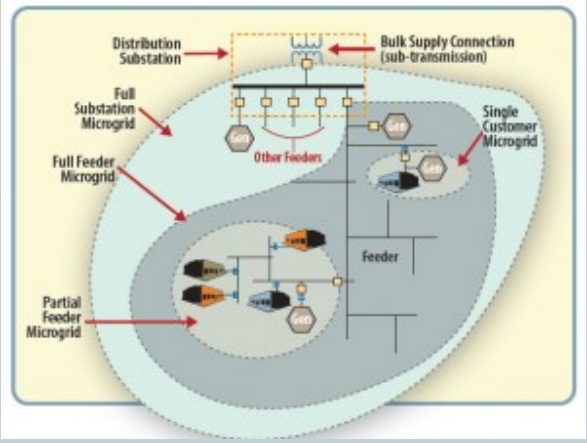


Diagram of the Energy Surety Microgrid™ developed by Sandia National Laboratory, which uses a new concept for energy generation and delivery systems. (Courtesy of Sandia National Laboratory/Released)

Backup diesel generators are the typical solution to the energy islanding need and work well for small installations (i.e., on a per-building basis). Microgrids are designed and managed to efficiently enable islanding across multiple generation resources and multiple buildings that can span an entire large base.

The capability to integrate multiple types of generation on the same microgrid also addresses another concern related to energy surety, the availability of fuel. Multiple generators can run on multiple types of fuel (i.e., a natural gas turbine and diesel generator on the same microgrid), allowing diversification of the supply chain in times of supply volatility. Microgrids are typically designed with a mind toward integrating renewable resources, such as wind and solar, which may not require imported fuels at all. [8]

Net Cost savings

Depending on the installation needs and the local utility environment, microgrids can in many cases save money over the course of a few years. There are three primary ways by which a microgrid can decrease operating costs, outlined as follows.

Generating power locally at a cost lower than the grid can supply it

Rooftop solar is now a familiar investment by businesses and consumers to offset their energy use and even sell low-marginal-cost power back to the grid via power purchase agreements with the local utility. Because microgrids can integrate those solar panels with generators, energy storage and other renewable resources in an intelligent, dispatchable fashion, they can increase the availability and quality of sellable power.

Solar panels installed on the roof of Space and Naval Warfare Systems Command Headquarters Old Town Complex in San Diego, California. (Photo by Rick Naystatt/Released)

The Advanced Metering Infrastructure (AMI) is already deployed across much of the United States and is equipped to perform near-real-time energy flow reporting to the utility and consumer via wired and wireless communications. Pending governing policy changes, this will likely more widely translate to real-time pricing structures per kilowatt-hour based on the current, live retail market price of energy. In this scenario, the microgrid has great flexibility in its choice of how to interact with the market. Its cost-based management algorithms can optimally balance its cost factors (efficiencies, capital depreciation, operations and maintenance, fuel, renewable resource forecast, storage cycling, etc.) and decide in near-real time whether to purchase or sell to the grid. It could feasibly even exercise energy arbitrage during periods of extremely high grid cost volatility.

Such energy demand/generation response also implicitly addresses the utility need for energy peak shaving, which serves to reduce the top capacity the grid infrastructure must be designed to handle. Large customers like military bases and factories are often charged additional infrastructure fees to offset the utility's cost to stand up

The Electric Microgrid— continued

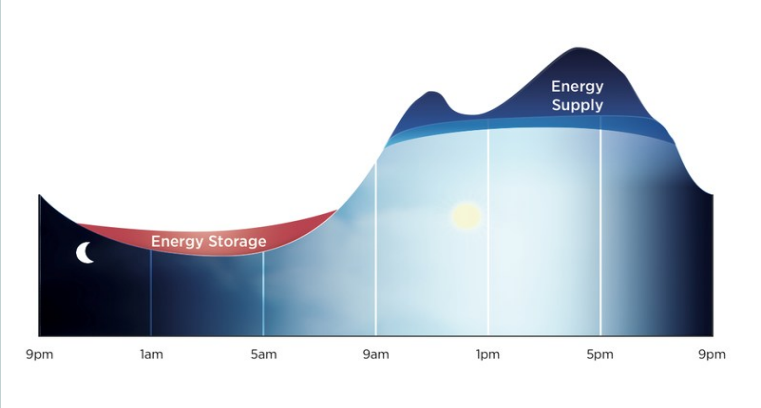
C. Doran

the fat distribution lines and substations needed to handle the large load peaks. By offsetting load peaks to the grid with local generation, the utility no longer needs the infrastructure-bolstering investment.

Selling ancillary services to the grid

Some energy services are even more valuable to the grid than active energy (i.e., kilowatt-hours). These are called ancillary services. The Federal Energy Regulatory Commission defines the ancillary services as "those services that are necessary to support the transmission of capacity and energy from resources to loads while maintaining reliable operation of the Transmission Service Provider's transmission system in accordance with good utility practice." [10] In order of value, the ancillary services worth most to the grid operator are regulation (voltage and frequency), spinning reserves and supplemental (non-spinning) reserves. [11]

The utility participates in high-value, fast-moving markets for these services, each of which can feasibly be provided by a microgrid. Regulation could be especially well-suited to be provided by inverters that can vary phase and frequency instantaneously. The ancillary services market attractiveness varies significantly from region to region, but it could prove a valuable income stream to the microgrid operator, especially as regulations move to support participation in these markets. [12]



A graph of peak shaving showing the utility's time-of-use rates. (Courtesy of http://en.openei.org/wiki//Released)

Improving efficiency of operations, especially when islanded

Microgrids allow significant optimization efficiency, both in grid-tied and islanded states. Consider even the specific simple case of traditional generators. Current backup generator systems are typically wired directly to critical load circuits, with a unique generator system for each building. This is not efficient use of fuel or capital, since each generator must operate at a very low load factor for the majority of operation time. If these multiple generators are networked across a broader microgrid instead, the load profiles are stabilized over a larger population. Now, generators can be selected and operated at optimal efficiency levels for their capacity with less volatility in load-tracking. Furthermore, redundancy in generators can be considered a shared resource across the entire microgrid instead of being required for each building; this reduces capital costs while maintaining the same reliability factor.

Forward-operating bases can be considered candidates of a special islanded-only application of microgrids. In recent conflicts, fuel resupply missions to these bases over mountainous terrain have been the cause of high casualty rates and high fully-burdened cost of fuel. When considering that electricity generation typically accounts for a large component of fuel use at camps and bases near the tactical edge, improving generation efficiency and integrating renewables via a microgrid architecture are highly valuable. [13]

Marines from 2nd Maintenance Battalion, 2nd Marine Logistics Group (Forward), escort more than 35 local national trucks to forward operating bases in northern Helmand province, Afghanistan, during a resupply mission June 30 through July 6, 2011. (Photo by Sgt. Rachael Moore/Released)

Combined Heat and Power (CHP) technology may be a particularly attractive option for microgrid generation at fixed installations from an efficiency standpoint. The efficiency of combustion generators is physically limited by the Carnot factor, which implies that waste heat will always be created. This waste heat can be captured and circulated to nearby buildings to serve many purposes, such as heating (air or water), cooling (via absorption processes) and air conditioning (via desiccation processes). By harvesting and distributing this heat energy directly, the total system efficiency (fuel conversion to electricity and heat to building) climbs from 45 percent to 80 percent.

The Electric Microgrid— continued

C. Doran

Heat vs electricity tuning has been shown to achieve a further 2-4 percent efficiency gain. Because heat transmission is limited in how far it can go, CHP plants are most effective when located close to the heat receiver. Microgrids encourage distributed generation and make CHP a more valuable option where its benefits might be realizable in a traditional grid with distant transmission. CHP is forecast to grow to 1.9 GW of installed base to represent $7 billion by 2018. [14]

In any discussion about the cost savings achievable by microgrids, one must also consider the costs for deployment. Upgrading an installation to a microgrid infrastructure will require a significant amount of initial capital to cover components and labor. Anyone planning to install a microgrid should consider the financing options that have emerged to address this issue. Utilities will often negotiate Power Purchase Agreements or Energy Service Agreements up-front to ensure adequate payback forecasts across long-term contracts. Other multi-party financial instruments include Enhanced Use Leases, Renewable Energy Service Agreements or Utility Energy Service Contracts. Additional procedural hurdles and costs must be fully understood if crossing military/federal/state regulators. [15]

"In any discussion about the cost savings achievable by microgrids, one must consider the costs for deployment."

Environmental

Microgrids enable high-penetration of distributed renewable resources. Renewables, such as solar and wind, are intermittent in nature, and because of their low power density and siting requirements, they must often be geographically distributed. This presents a challenge to the traditional radial grid architecture, but microgrids have active control mechanisms and typically incorporate storage to offset intermittency effects. By connecting the microgrid's locally-aggregated and stabilized renewable generation to the main grid via a controlled single Point of Common Connection, the grid is able to accommodate a higher penetration of renewables without the stability concerns typically caused by distributed renewables.

The National Defense Authorization Act of 2007 requires that 25 percent of all energy consumed from DoD installations be renewable by 2025, and many branches of the DoD have followed-up with their own energy efficiency and renewability goals. [16] Microgrids are an effective way to help meet or exceed these goals. This is important given the DoD's vast electricity expenditures, $4 billion to power 300,000 buildings at 500 installations globally, and domestic bases will likely only increase demand as troops return home from conflicts abroad. [17]

Microgrid systems are currently the only solution that allows the incorporation of multiple technologies, such as renewables and energy storage systems, to supplement traditional power generation techniques. (Photo by Spc. Robert Porter/Released)

Case Studies

For a detailed survey of 44 studied, planned or installed microgrids at DoD installations up through mid-2012, the reader is encouraged to read ref. [11]. This section will provide some updates to those reports and describe a few notable newer and non-DoD examples.

The Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) microgrid project led by Sandia National Laboratories has completed phases 1-2 at Fort Carson, including a 72 hour plug-in electric vehicle demonstration. The next phase is at Camp Smith and will feature an entire cyber-secure 5 MW installation with high-penetration renewables, demand -side management and redundant backup. A co-developed product of the SPIDERS project is Sandia's Microgrid Cyber Security Reference Architecture, which lists best practices for securing control systems in a microgrid. [15]

Forward Operating Bases may be important applications of microgrid technology in coming years. A recent simulation based on observed load data from a base in Afghanistan showed that microgrids powered by Advanced Medium Mobile Power Sources and multiple Tactical Quiet Generators can save 16 percent of fuel and reduce net operating hours by 54 percent, which reduces maintenance needs. [18]

The Electric Microgrid— continued

C. Doran

"The National Defense Authorization Act of 2007 requires that 25 percent of all energy consumed from DoD installations be renewable by 2025…"

The University of California, San Diego operates a large 42 MW microgrid with photovoltaic, fuel cell, and combined heat and power generation. It is considered one of the most efficient microgrids in the country, and the university reports saving $800,000 per month on energy expenditures after an initial investment of $8 million. The microgrid performed islanded operation during a large blackout event across Southern California, Arizona and Mexico in 2011. **Princeton University** has also demonstrated islanding of their smaller but similar 15 MW microgrid, which continued operating through outages caused by Superstorm Sandy in 2012, as did the Food and Drug Administration's White Oak research facility, which has a large combined heat-and power plant. [19]

The Galvin Electricity Initiative has been active in microgrid demonstration projects, including demonstrators at Bella Coola, British Columbia and the Illinois Institute of Technology. The former demonstrated a 64 percent diesel use reduction by adding hydrogen storage to a diesel and hydroelectric microgrid. The latter includes real-time energy pricing communications to loads.

The Consortium for Electric Reliability Technology Solutions (CERTS) developed one of the first highly-publicized microgrids, which has become a model for the industry. The test bed incorporates synchronous and photovoltaic generation, load shedding, storage and intelligent energy management control. The microgrid has demonstrated it can achieve stable islanding and resynchronization without any high-speed communications between generators, and it is capable of handling inductive loads and internal faults. [20]

The Twenty-nine Palms Marine Corps Air Ground Combat Center microgrid installation introduced in the MIT Lincoln Labs study has since added 5 MW of photovoltaics, 500 kW of batteries, and a new 8 MW combined heat and power plant that accompany the existing plant. It continues to be successful in its mission of improved efficiency, reliability and environmental friendliness. [21]

Conclusions

Microgrids provide an architecture for electricity surety by enabling seamless transitions from grid-tied to self-sufficient islanded operation that can generate electricity from a variety of resources and fuels. Because they include an automated management element that communicates with its distributed resources and the utility in a location-based manner, microgrids can achieve a higher efficiency than is often possible with building-specific backup generators or even the conventional grid in many cases. Finally, in part because of that management element, microgrids enable the high-penetration insertion of renewable resources in a way that is not feasible with traditional backup systems or centralized grids.

Buoyed by investments in Smart Grid initiatives, microgrid technology has advanced rapidly in the past decade in technology readiness as simulations and lab demonstrations move to live pilot installations that support live critical loads. Some of these installations have had the opportunity to prove their worth when tested against real-world blackouts from weather-caused and utility-caused blackouts.

CERDEC demonstrated a proof of concept for a smart grid that could support tactical operations this summer at its integrated capabilities test-bed at Fort Dix, N.J. (Photo by Spc. Robert Porter/Released)

The Electric Microgrid— continued

C. Doran

About the Author:

Mr. Chris Doran supports the HDIAC on behalf of Northrop Grumman Corporation to contribute subject matter expertise for Alternative Energy. He earned a B.S. in Electrical Engineering and an M.S. in Nanoelectronics with a focus on Energy Materials from the University of California, San Diego. His background includes laboratory research in nanoelectronics and flexible photovoltaics, as well as systems engineering for electric utility and defense industries.

References:

[1] Environmental Security Technology Certification Program. "Smart Microgrid Energy Management Controls for Improved Energy Efficiency and Renewables Integration at DoD Installations," 2013.

[2] Department of Energy Microgrid Exchange Group.

[3] Consortium for Electric Reliability Technology Solutions (CERTS). "Integration of Distributed Energy Resources. The CERTS MicroGrid Concept. Consultant Report." California Energy Commission, 2003.

[4] J. D. Guggenberger. "Performance Characterization And Optimization Of Microgrid-based Energy Generation And Storage Technologies." Missouri University of Science and Technology, 2012.

[5] U.S. Department of Energy, Energy Information Administration, 2013.

[6] L. Tao, et al. "From Laboratory Microgrid to Real Markets – Challenges and Opportunities." 8th International Conference on Power Electronics - ECCE Asia, 2011.

[7] R. W. Galvin, K. E. Yeager. "Perfect Power: How the Microgrid Revolution will Unleash Cleaner, Greener, and More Abundant Energy." McGraw-Hill, Inc., 2008.

[8] S. B. Van Brockhoven, et al. "Technical Report 1164. Microgrid Study: Energy Security for DoD Installations." Lincoln Laboratory Massachusetts Institute of Technology, 2012.

[9] M. Hightower. "Energy Surety Microgrids™ for Critical Mission Assurance to Support DOE and DoD Energy Initiatives." Energy Systems Analysis Department, Sandia National Laboratories.

[10] FERC Order 888-A, April 1996.

[11] Y. Xiao (ed). "Communication and Networking in Smart Grids." CRC Press. 2012.

[12] Federal Energy Regulatory Commission Staff. "Payment for Reactive Power Commission Staff Report," 2014.

[13] Army Environmental Policy Institute. "Sustain the Mission Project: Casualty Factors for Fuel and Water Resupply Convoys Final Technical Report," 2009; P. Asmus, K. Adamson. "Military Microgrids Stationary Base, Forward Operating Base, and Mobile Smart Grid Networks for Renewables Integration, Demand Response, and Mission-Critical Security." Pike Research, 2012.

[14] Reliability Information Analysis Center (RIAC). "Assessment of Microgrid Applications to Tactical Edge Military Operations." Technical Report: RIAC TAT Number – RI-12-RMS#117/DO#203, 2013.

[15] C. K. Veitch, et al. SAND2013-5472 "Microgrid Cyber Security Reference Architecture." Sandia National Laboratories, 2013.

[16] Environmental and Energy Study Institute. "DoD's Energy Efficiency and Renewable Energy Initiatives," 2011.

[17] Installations and Environment. "Department of Defense Annual Energy Management Report Fiscal Year 2013," 2014.

[18] U.S. Army Materiel Systems Analysis Activity. Technical Report No. TR-2014-04. "AMSAA Analysis of Project Manager Mobile Electric Power Operational Energy Solutions in Afghanistan "Operation Dynamo II," 2014.

[19] J. St. John. "How Microgrids Helped Weather Hurricane Sandy." Greentech Media. https://www.greentechmedia.com/articles/read/how-microgrids-helped-weather-hurricane-sandy, 2012.

[20] J. Eto, et al. "Overview of the CERTS Microgrid Laboratory Test Bed." CIGRE2009 (2009); CERTS Microgrid Phase Two Test Report.

[21] U.S. Department of Defense Environmental Security Technology Certification Program. ESTCP Cost and Performance Report (EW-200937): "Smart Microgrid Energy Management Controls for Improved Energy Efficiency and Renewables Integration at DoD Installations," 2013; K Kaufmann. "Twenty-nine Palms co-gen plant aims for efficiency." The Desert Sun. 30 March 2014. http://www.desertsun.com/story/tech/science/energy/2014/03/29/twentynine-palms-co-generation-power-plant/7069857/.

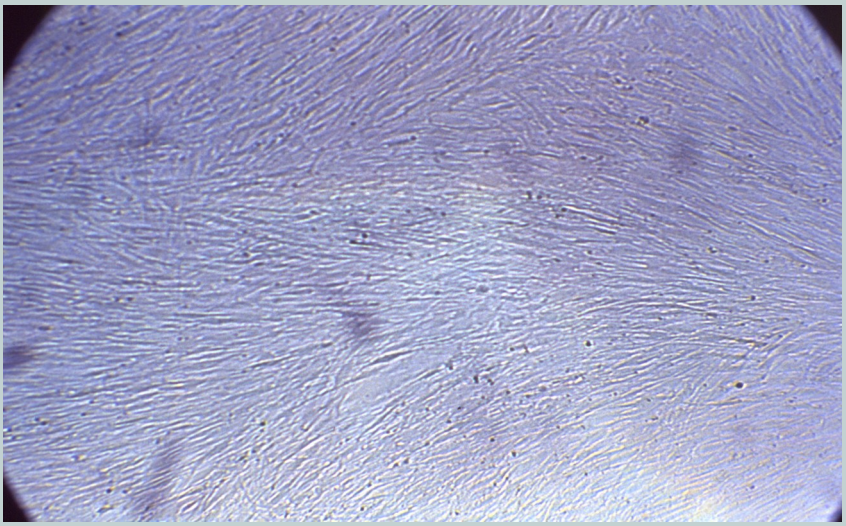
Technical Inquiry Highlight

The Technical Inquiry Highlight for this issue is an inquiry from a government agency requesting information on more efficient, effective alternative techniques for drug testing. They were particularly interested in information that enumerated various testing approaches, where the approaches are being used, data on the effectiveness of the approaches and the expected outcomes.

The current protocol in pharmaceutical and toxicology science is *in vivo* testing, which begins with animal testing and then moves on to human clinical trials. In the early phases of drug development, animal models have previously been the only way to obtain *in vivo* data that can potentially predict the human pharmacokinetic response. However, there are concerns about the validity of animal models because of the deficiency in cross-species extrapolation. Currently, 9 out of 10 trials that go through animal testing fail during human trials. With 90 percent of new compounds failing in human trials and billions of dollars being spent, the development of an improved method for drug testing is very important.

The inquiry report provided the agency with a broader understanding of *in vitro*, *in silico*, stem cell research, organs-on-a-chip and the institutes that are developing alternatives to animal testing. The Wyss Institute at Harvard University is the lead developer of human-on-a-chip technology. The Institute works with pharmaceutical companies to design drug tests that use organ tissue to observe the mechanisms of both disease and drug interactions. These tissue/organ chips can be used to rapidly assess responses to new drug candidates, providing critical information on the safety and efficacy of the new drugs. Another institute utilizing these alternative techniques is the U.S. Army Research Laboratory, Edgewood Chemical and Biological Center (ECBC), where researchers are examining exposure of various chemicals, pharmaceuticals and chemical warfare agents on specific human organs via organs-on-a-chip technology.

The customer was provided the requested information, which was reviewed and approved by an HDIAC SME. This stimulated additional discussions, resulting in the direct connection of the HDIAC SME and customer for additional consultation and information. With the information provided by the HDIAC team and the SME network, the customer was able to make an informed decision on a path forward for future endeavors.



Human Embryonic Lung Fibroblasts (HELF) cells. (Courtesy of Centers for Disease Control and Prevention (CDC), Susan Lindsley/Released)

Coming up next issue...

Cultural Studies

Army Social Science Lessons for Homeland Defense Planning and Operations

How do we meet the challenges operational and strategic environments pose? In this article, the author proposes that part of the answer is found in the lessons learned from the Army's use of Human Terrain Teams (HTT). Seven years of deployed social science show that obtaining accurate, timely and relevant sociocultural insight to use in planning processes requires researchers working with the population in question and alongside security personnel responsible for a given area. The level of accuracy and relevance needed in regards to cultures cannot be obtained from computer simulations, remote sensing systems and reach-back centers, or by sifting through documents and reports on a hard drive or the internet. Social science support for planning, decision-making and developing a shared understanding of the human domain requires being in the field. This equates to interdisciplinary social science teams conducting research among the population and interacting with stakeholders on the ground. This article will detail the author's experiences with HTT and provide examples of the application of social science in a military setting.

Medical

Ebola

Ebola Hemmorhagic Fever (Ebola HF), or Ebola Virus Disease (EVD), is a severe and often fatal viral hemmorhagic fever disease of humans and other primates. Case fatality rates vary from 50 to 90 percent in humans. The name "Ebola" recognizes the 1976 discovery of Ebolavirus near the Ebola River (two simultaneous outbreaks: Nzara, Sudan and Yambuku, Democratic Republic of Congo). Periodic outbreaks of the disease, suggesting crossover into a new human host from a natural reservoir (which may include indigenous bat populations), have been observed since that time, leading up to the most severe outbreak on record, which currently involves populations in Guinea, Liberia, and Sierra Leone. Ebola HF illustrates an important insight in medical virology, the most pathogenic viral infections are often associated with recent inter-species crossover from an evolved and adapted host-viral interaction (Ebola virus – Bat) to infection of a new host (Ebola virus – Human). This article will give an overview of the history of the disease and the 2014 outbreak.

Coming up next issue...

Homeland Defense and Security

Advances in Explosive Trace Detection Technology

It is widely acknowledged that the greatest terrorism threat to homeland security in western countries in the coming years is posed by foreign fighters returning from conflicts such as those in Syria and Iraq. These hardened extremists will bring with them hard-line beliefs and training in fabricating and employing explosives to achieve maximum effect. It is also likely many of these returning fighters will have had training in devices designed to avoid detection.

Perhaps one of the most understated attractions of 'home-made' explosives for terror cells is that many of these types of explosives currently fall within the grey area of what can be accurately identified by current explosive trace detection technology. Presently, most inorganic salts and peroxides cannot be identified by the same detection unit, which potentially increases the likelihood of successfully smuggling the dangerous substance through screening areas.

Recently, a team at the University of Tasmania in Australia developed leading technology innovation for the next generation of explosive trace detection equipment. This technology can identify military and commercial grade explosives and both inorganic and peroxide molecules found in many 'home-made' explosives. The key breakthrough of this technology is its ability to accurately and consistently detect trace quantities of inorganic explosives within 60 seconds, a world first for trace detection technology.

Critical Infrastructure Protection

A Primer on the Defense Industrial Base

This is the third in a series of articles for the Homeland Defense and Information Analysis Center (HDIAC) describing the fundamental directives and charters that provide our Nation's strategy for Homeland Defense and Security as well as the DoD's role in supporting the National Infrastructure Protection Plan (NIPP). This article will describe the DoD plan for protecting our Critical Infrastructure as the Sector–Specific lead for the Defense Industrial Base (DIB).

HDIAC Calendar of Events

2015 AFCEA Homeland Security Conference
10-12 March 2015
Washington, DC

Maritime Security 2015 East
10-12 March 2015
Jacksonville, FL

31st Annual National Logistics Forum
16-18 March 2015
Washington, DC

Satellite 2015
16–19 March 2015
Washington, DC

Precision Strike Annual Review (PSAR-15)
17-18 March 2015
Springfield, VA

Globalcon 2015
17-18 March 2015
Philadelphia, PA

Medical Research, Development and Acquisition in Support of the Warfighter
23-25 March 2015
College Park, MD

2015 Joint Summits on Translational Science
23-27 March 2015
San Francisco, CA

Future Artillery 2015 – Taking Firepower Forward
24-25 March 2015
London, UK

16th Annual Science and Engineering Technology Conference
24-26 March 2015
Springfield, VA

Experimental Biology 2015
28 March – 1 April 2015
Boston, MA

American Society for Industrial Security (ASIS) International European Security Conference and Exhibition
29-31 March 2015
Frankfurt, Germany

Noteworthy

Alternative Energy

Researchers discover new material to produce clean energy
March 3, 2015

Na-ion batteries get closer to replacing Li-ion batteries
March 3, 2015

Big box stores could ditch the grid, use natural gas fuel cells instead
March 4, 2015

Biometrics

New algorithms locate where a video was filmed from its images and sounds
February 16, 2015

Cross-cultural communication: Much more than just a linguistic stretch
February 24, 2015

CBRN Defense

Silver lining for paper Ebola test
February 17, 2015

Researchers use lab-scale human colon and septic tank to study impact of copper nanoparticles on the environment
March 2, 2015

DHS termination of bio-detection contract questioned
March 4, 2015

Critical Infrastructure Protection

A new level of earthquake understanding: Surprise findings from San Andreas Fault rock sample
March 3, 2015

Terrorists shift focus of attacks from air transportation to rail systems
March 4, 2015

Noteworthy

Cultural Studies

Jordan's illegal labor puzzle: Let Syrian refugees work or just survive?
March 2, 2015

An Inhumane Trade: Partnering against Human Trafficking
March 5, 2015

Homeland Defense and Security

Laser weapon system stops truck in field test
March 4, 2015

Flood and drought risk to cities on rise even with no climate change
March 5, 2015

Medical

Link between inflammation, tissue regeneration and wound repair response
February 25, 2015

Cerebral blood flow as a possible marker for concussion outcomes
March 2, 2015

Vaccines from a reactor
March 2, 2015

Weapons of Mass Destruction

U.K. military examined feasibility, impact of terrorists using weaponized Ebola virus
February 10, 2015

WEST: NORAD Head Says Russia Increasing Arctic Long Range Air Patrols
February 10, 2015

The Homeland Defense & Security Information Analysis Center (HDIAC) is a Department of Defense (DoD) Information Analysis Center (IAC) providing scientific and technical information (STI) to the homeland defense and security communities.

HDIAC is managed by the DoD IACs Program Management Office (PMO) through the Defense Technical Information Center (DTIC).

DoDIACs

Department of Defense Information Analysis Centers

http://iac.dtic.mil/

CSIAC
Cyber Security & Information Systems Information Analysis Center

DSIAC
Defense Systems Information Analysis Center

HDIAC
Homeland Defense & Security Information Analysis Center

Contact Us
Homeland Defense & Security Information Analysis Center
104 Union Valley Road
Oak Ridge, TN 37830
(865) 535-0088 (phone)
(865) 481-0390 (fax)
www.hdiac.org

M. Freiderich, Managing Editor
mfreiderich@hdiac.org or (865) 813-1075