CENTER for STRATEGIC LEADERSHIP and DEVELOPMENT CSLD U.S. ARMY WAR COLLEGE

Issue Paper

Center for Strategic Leadership and Development
U.S. Army War College

THE UNITED STATES ARMY WAR COLLEGE STRENGTH and WISDOM

Volume 1-13, October 2013

TERMINAL BLACKOUT: CRITICAL ELECTRIC INFRASTRUCTURE VULNERABILITIES AND CIVIL-MILITARY RESILIENCY

Cynthia E. Ayers & Kenneth D. Chrosniak

The U.S. Army War College is "an educational institution focused on its students and dedicated to Landpower's role in national security; ready to challenge assumptions and conventional wisdom; ready for any mission from fellow Soldiers; and in the war of ideas – always looking for a fight. "

—Major General Tony Cucolo, Commandant, United States Army War College

CLEAR AND PRESENT DANGER

Threats to the electric grid (cyber, solar, non-nuclear electromagnetic pulse [NNEMP] and high-altitude nuclear electromagnetic pulse [HEMP]), as well as the potential consequences of significant damage to grid components by terrorists and other natural disasters, have increased incrementally since 2001; but details releasable to the public at the unclassified level were rare prior to 2008. Efforts by the Congressional *Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP Attack)* to declassify data relevant to American society within their final 2008 report were successful[1] (albeit limited, as much remains classified), and subsequently heralded during a major conference at Niagara Falls,[2] sponsored by a new non-profit non-partisan organization,[3] which hosted highly influential experts and proponents of critical electric infrastructure protection. Participants included sitting and retired Congressional members from both parties; former Directors of the CIA, the National Security Agency, and the Defense Nuclear Agency; counterterrorism analysts; commissioners; nuclear and electrical engineers; scientists; academics; and a wide variety of first responders.

The *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP Attack): Critical National Infrastructures*,[4] the proceedings of a National Academy of Sciences workshop entitled *Severe Space Weather*

1. John S. Foster, Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood, Jr., and Joan B. Woodard, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (Washington, D.C.: EMP Commission, April 2008), http://www.empcommission.org/docs/A2473-EMP_Commission-7MB.pdf (accessed August 12, 2013).
2. EMPact America, Inc, *Permanent Continental Shutdown From Electromagnetic Pulse: A National Conference on the EMP Threat* (September 8-10, 2009), (Niagara Falls, NY: EMPact America, Inc., September, 2009).
3. EMPact America Homepage: http://www.empactamerica.org/videos_conference.php (accessed September 14, 2013).
4. Foster et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*.

Cynthia Ayers is a consultant in the Mission Command and Cyber Division (MCCD) of the Center for Strategic Leadership and Development (CSLD).

Ken Chrosniak is an education specialist in MCCD, CSLD.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
OCT 2013		**00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Terminal Blackout: Critical Electric Infrastructure Vulnerabilities and Civil-Military Resiliency	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army War College,Center for Strategic Leadership and Development,650 Wright Avenue,Carlisle,PA,17013-5049**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

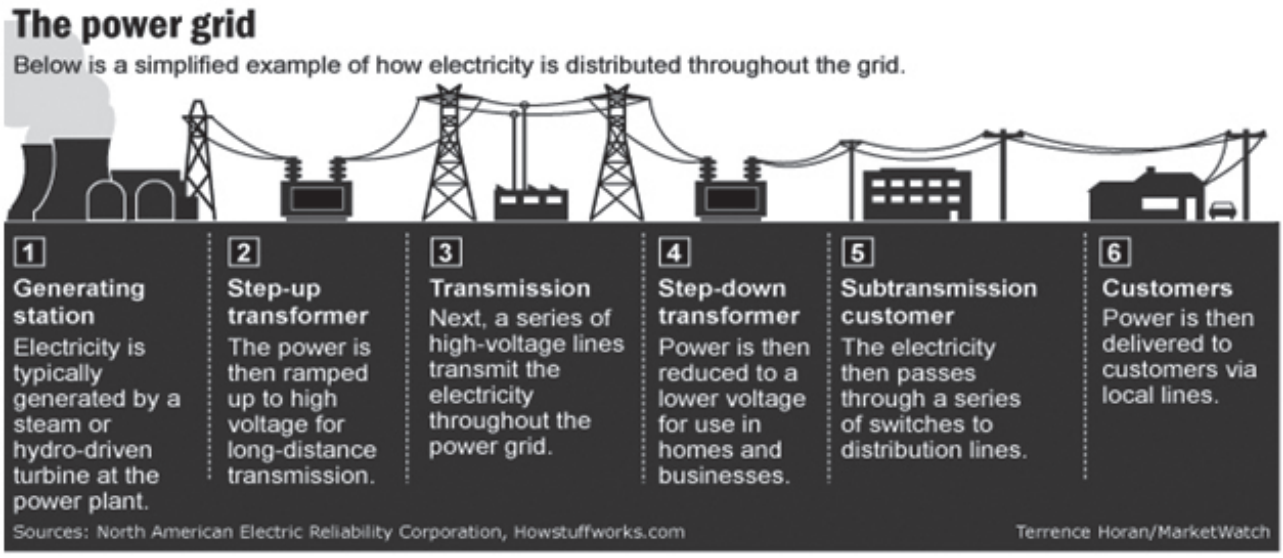
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**8**	



Grid vulnerable at all points of distribution; but most crucial to harden is 1, 2 and 4.

Events: Understanding Societal and Economic Impacts,[5] a series of Metatech Corporation research publications,[6] and several other official documents written within approximately the same timeframe (2008-2010), all noted the extremely vulnerable state of our electric grid to high-altitude nuclear detonations, great geomagnetic storms (from Coronal Mass Ejections [CMEs]), and cyber attack. They stated that these events would result in extensive outages ("months-to-years"[7] and "4 to 10 years"[8]), the cascading collapse of virtually all other critical infrastructures, and potentially the loss of over 2/3rds of our population from starvation, civil disorder, and disease.[9]

The extended loss of electric power is our nation's most glaring national security "Achilles Heel." Energy is the overarching component of all the sectors which comprise the strength and vitality of America—it is the blood within the circulatory system that makes everything run. If you remove energy from the mix, the rest of the structure will buckle and ultimately break down.

Thus, "the current vulnerability of U.S. critical infrastructures can both invite and reward attack if not corrected."[10] Considering the unprepared state of the grid, a single attack could remove the United States as an actor on the world stage, instantaneously and long-term. Our enemies already know this. They discuss it openly, and have embedded it within their doctrine, while preparing for the possibility of such an attack on their own energy grid and communication systems.

A single attack could remove the United States as an actor on the world stage, instantaneously and long-term.

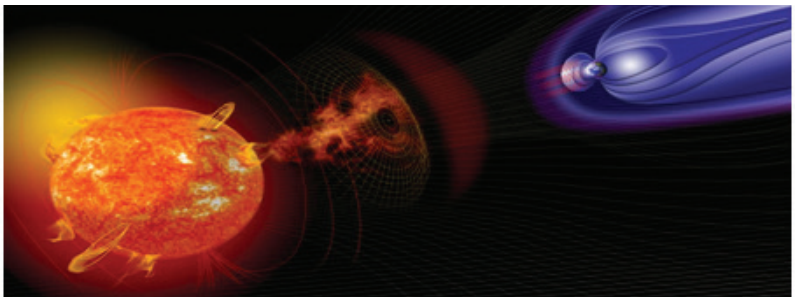
WHEN PLANNING, ALWAYS PLAN WORST CASE

The worst case scenario was eloquently described by the Assistant Secretary of Defense for Homeland Defense/ America's Security Affairs, Dr. Paul Stockton, during his presentation to the graduating U.S. Army War College's

5. The National Research Council, *Severe Space Weather Events: Understanding Societal and Economic Impacts* (Washington DC: National Academies Press, 2008) http://books.nap.edu/catalog.php?record_id=12507 (accessed August 12, 2013).
6. John Kappenman, William Radasky, Edward Savage, James Gilbert, *Electromagnetic Effects on the U.S. Power Grid* (a.k.a. "The Oakridge Study" encompassing META-R-319 through META-R-324) (Goleta, CA: Metatech Corporation, January 2010).
7. Foster, et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, 30.
8. The National Research Council, *Severe Space Weather Events: Understanding Societal and Economic Impacts*, 4.
9. Peter V. Pry, *Statement Before the Congressional Caucus on EMP*, February 15, 2011, http://www.empactamerica.org/pry-statement-to-emp-caucus.pdf (accessed August 11, 2013).
10. John S. Foster, Jr., Earl Gjelde, William R. Graham, Robert J. Hermann, Henry M. Kluepfel, Richard L. Lawson, Gordon K. Soper, Lowell L. Wood, Jr., and Joan B. Woodard, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume. 1: Executive Report* (Washington DC: EMP Commission, 2004), 3.

(USAWC) Distance Education class on 24 July 2012.[11] Dr. Stockton addressed the issue of massive and cascading loss of the electric grid, emphatically reiterating the dire warnings of the EMP Commission report, in which HEMP, geomagnetic disturbances (GMD), coordinated physical and cyber attacks, earthquakes and other natural disasters could take down the grid. (A video of his briefing is available at: http://www.youtube.com/watch?v=Frgxuc1fkDg. Advance the video to the 10 minute mark to see Dr. Stockton's introduction.)

Catastrophic critical infrastructure failure is the epitome of "worst case." A burst of high-intensity electromagnetic radiation generated by a high-altitude explosion will damage and disrupt electronics and electrical systems within an area defined by line-of-sight from the blast, potentially cascading to other critical sectors such as transportation, chemical, dams, emergency services, food and agriculture, information technology, financial services and more. A suddenly fluctuating magnetic field generated by a direct hit from a Coronal Mass Ejection (CME) will achieve similar results in which the blackout could reach far beyond the normal boundaries of large-scale complex natural catastrophes (such as Hurricanes Katrina and Sandy or the earthquake and tsunami that devastated Japan in 2011) and last much longer with more devastating repercussions.



A National Academy of Sciences report "estimated that about 365 critical [extra-] High Voltage (EHV) transformers in the continental United States are at risk of failure or permanent damage requiring replacement in the event of a solar superstorm."[12] These transformers are critical to civilian communities, military installations, and the Defense Industrial Base. Estimates for on-hand spare EHV transformers are generously considered to be approximately 2% (nation-wide), as each is unique, costly, and can take up to two years to build. Furthermore, "replacing damaged transformers is a major logistical undertaking, with a typical high-voltage transformer about as big as a small house and weighing 500,000 pounds (227 metric tons)."[13] Replacement of several transformers simultaneously would be impossible in the short-term and extremely problematic in the long-term, as most are manufactured overseas. With a significant storm, the potential exists for thousands of transformers to go into "melt-down" condition, and recovery would be long-term indeed. The National Academy of Sciences estimate of 4 to 10 years is considered a "conservative" estimate by many experts,[14] not only because of manufacturing difficulties, but also because of the need for specially built trains and trucks for transport, as well as the need for improvements or restructuring of roads and bridges to accommodate the tremendous size and weight of the transformers.

Depending on weapon design and delivery method (if caused by intentional attack), or on the strength, nature, and direction of an earth-bound CME, smaller electronics—such as those used in transportation and health systems—could also be damaged. Transportation, communications, financial transactions, food production and a multitude of other functions would eventually (if not simultaneously) come to a halt. Fukushima-like events could follow outages at nuclear power plants, considering a low probability of there being sufficient on-site capability to maintain the cooling systems for the spent fuel-rod pools longer than a month.[15]

A catastrophic nationwide HEMP would only require a kiloton-sized warhead, if the design is that of an "advanced" or "super-EMP" weapon, detonated approximately 300 miles over the middle of the nation, such as over Missouri. Alternatively, a nuclear-tipped missile with even a basic guidance system, fired off the coast of New York, could take down the entire northeastern portion of the grid, and initiate a cascading effect across the country. Three missiles

11. Paul Stockton, ASD (HS/ASAA), "Strategic Challenges for Warfare," speech, U.S. Army War College, Carlisle Barracks PA, July 24, 2013, cited with permission of Dr. Stockton: www.youtube.com/watch?v=Frgxuc1fkDg (accessed September 18, 2013).
12. Deborah Zabarenko, "Solar Superstorm Could Knock Out US Power Grid-Experts," *Reuters*, August 3, 2012 http://www.reuters.com/article/2012/08/04/us-solar-superstorm-idUSBRE8721K820120804 (accessed August 28, 2013).
13. Ibid.
14. The National Research Council, *Severe Space Weather Events: Understanding Societal and Economic Impacts,* 4.
15. Thomas S. Popik, *Protecting Spent Fuel Pools at Nuclear Power Plants from Long-Term Loss of Outside Power*, Foundation for Resilient Societies, http://www.tisp.org/index.cfm?pk=download&pid=10261&id=13150 (accessed September 16, 2013).

specifically launched to take down each of the three main sectors of the grid would virtually guarantee an extensive outage over a vast area with devastating effects.

A well-conceived and well-coordinated cyber-attack could also achieve many of the same effects, as noted by a former Director of the CIA,[16] the former Secretary of Homeland Security,[17] a former Secretary of Defense,[18] and the President himself.[19] Chinese preparations for a cyberwar include "soft" and "hard" kill options for network communications and critical infrastructure. "Soft-kill" attacks include disruption and damage using cyber hacking and infiltration, while "hard-kill" cyber-attacks are notably radio frequency weapons and missile delivery systems.[20] A recently reported cyber infiltration of a "honeypot" (a decoy) water SCADA (supervisory control and data acquisition) system by hackers believed to be associated with the Chinese Army could be indicative of things to come.[21]

Chinese Cyber Hackers

Kinetic attacks on the electric grid as a means to bring down other Critical Infrastructure/Key Resources (CI/KR) have been noted in written work and interviews of senior government and military officials of Iran, North Korea, China, and Russia, and in some cases discussed within the context of preemptive first strike capabilities.[22] If the United States should fall victim to a preemptive strike on its electric grid, retaliation in kind would be irrelevant, since these countries are known to be hardening their own infrastructures; and, of course, if the perpetrator is the sun, there won't be anyone to retaliate against anyway! Ultimately, in the event of a large-scale CME or an attack (via cyber warfare or high-altitude nuclear detonation) by adversaries knowledgeable of grid vulnerabilities, hundreds of millions would have to learn to survive without electricity or face the deadly consequences.[23]

THREAT TO THE HOMELAND

These clear and present dangers to America, and specifically to the U.S. Army, exist right now with the likely degradation or loss of vital commercial electric AC power which supports military installations, the Defense Industrial Base, and particularly the critical supply-chain. This has been clearly confirmed by past Secretary of Defense, Leon Panetta; retiring Secretary of Homeland Defense, Janet Napolitano; the 2004 and 2008 Congressional EMP Commission reports; NASA Goddard Space Center; the Federal Electric Reliability Commission (FERC); and the North American Electric Reliability Corporation (NERC). In personal correspondence between Dr. Stockton and personnel from the USAWC's Mission Command and Cyberspace Division (MCCD), Dr. Stockton stated that the loss of the electric

16. Paul D. Shinkman, "Former CIA Director: Cyber Attack Game-Changers Comparable to Hiroshima," *U.S. News and World Report*, February 20, 2013 http://www.usnews.com/news/articles/2013/02/20/former-cia-director-cyber-attack-game-changers-comparable-to-hiroshima (accessed August 28, 2013).
17. Ray Suarez, "Examining Cyber Security With Homeland Security Secretary Janet Napolitano," *PBS Newshour*, February 15, 2013 http://www.pbs.org/newshour/bb/science/jan-june13/cybersecurity_02-15.html (accessed February 26, 2013); Tony Romm, "Janet Napolitano warns of cyberattack on utilities," *Politico,* November 1, 2012, http://www.politico.com/news/stories/1012/83124.html?hp=r9 (accessed November 1, 2012).
18. Jake Tapper, "Leon Panetta: A Crippling Cyber Attack Would Be 'Act of War'," *ABC News*, May 27, 2012, http://abcnews.go.com/blogs/politics/2012/05/leon-panetta-a-crippling-cyber-attack-would-be-act-of-war/(accessed August 28, 2013).
19. The White House, *Remarks by the President in the State of the Union Address*, February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/remarks-president-state-union-address (accessed February 13, 2013); The White House, *Presidential Policy Directive – Critical Infrastructure Security and Resilience* (PPD-21), February 12, 2013, http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (accessed August 29, 2013).
20. Bill Gertz, "China's Military Preparing for 'People's War' in Cyberspace, Space," *The Washington Free Beacon*, July 30, 2013 http://freebeacon.com/china-military-preparing-for-peoples-war-in-cyberspace-space/ (accessed 23 August 2013).
21. Tom Simonite, "Chinese Hacking Team Caught Taking Over Decoy Water Plant," *MIT Technology Review* (online), August 2, 2013 http://www.technologyreview.com/news/517786/chinese-hacking-team-caught-taking-over-decoy-water-plant/ (accessed August 30, 2013).
22. Peter V. Pry, *Statement Before the United States Senate Subcommittee on Terrorism, Technology, and Homeland Security Hearing on Terrorism and the EMP Threat to Homeland Security: "Foreign Views of Electromagnetic Pulse (EMP) Attack,"* March 8, 2005, http://www.gpo.gov/fdsys/pkg/CHRG-109shrg21324/pdf/CHRG-109shrg21324.pdf, p 46 (accessed September 8, 2013).
23. Peter V. Pry, *Statement Before the Congressional Caucus on EMP*.

grid "keeps him awake at night." That exact sentiment was recently and publicly echoed by a highly placed Cyber Command (CYBERCOM) officer while discussing a HEMP detonation over the central part of America.

In an 11 September 2013 Senate Homeland Security and Governmental Affairs hearing, retired U.S. Coast Guard Admiral Thad Allen noted that there is a need for "a coherent document for managing large complex emergencies that would require the involvement of many departments." Homeland Security Policy Directive 5 (HSPD 5) specifies that the Secretary of DHS is responsible for the management of incidents domestically, but "frankly, when we have these large complex events, it's very hard to suborn one department to another," Admiral Allen said. He then noted that such disasters will probably get "more complex…[with] the possibility of a cyber attack triggering a kinetic effect," [24] thereby validating the importance of targeted and viable Cyber research and wargames being performed at the Center for Strategic Leadership and Development (CSLD).

CONSEQUENCES

The DoD infrastructure is dependent on continuous and assured 'outside the wire' AC power to support its varied missions for CONUS and OCONUS expeditionary operations. As Dr. Stockton stated in his USAWC presentation: "The smart thing to do is to maneuver around those forces, attack the critical infrastructure, the facilities here in the United States on which we depend to deploy, operate and sustain our forces abroad."[25] This way they avoid attacking the pointy end of the spear – direct military confrontation – in favor of softer U.S. domestic non-military targets.

Since our military facilities rely heavily on commercial electricity from and through the surrounding communities, personnel who are assigned to and work on military installations would be no better off than the civilians within these stricken areas. Catastrophic critical infrastructure failure within a large geographic area would immediately result in degradation (or termination) of the Army's ability to conduct unified landpower operations overseas, and would negatively affect the ability to respond to subsequent follow-on attacks, as there would be limited maneuver and communicative capabilities both CONUS and OCONUS.

The Defense Support to Civilian Authorities (DSCA) response to such a scenario would depend largely on the mode of attack and/or the severity of the event in that mission command, communications, and transportation could be severely impacted. A space-based HEMP could disable satellites, severely impacting civilian and military command and control.[26] Regardless, civilians will inevitably migrate to the closest military installation, expecting support in the form of food, water and protection; just as civilians long ago sought safety within the structure of military fortifications. Because all facilities are now resourced using supply-chain practices and "just-in-time" logistics, civilians can no longer be assured of such support from military installations. They would be no more effective under these circumstances than a mirage in the desert. Compounding this further is the fact that there has been virtually no testing or training for catastrophic critical infrastructure failure. There are no known scenarios, exercises or plans developed to date which encompass a complex catastrophe over several regions simultaneously, in which there is significant degraded or denied space for military DSCA operations.

RESPONSE: MCCD ACTIONS AND INITIATIVES

Personnel from the MCCD and CSLD have spent nearly five years working various aspects of these threats; however much remains to be done to attain even a limited amount of resilience within the Homeland. To effect needed change, MCCD representatives have developed working relationships with members of the Congressional EMP Commission; the Congressional EMP Caucus (chaired by Congressman Trent Franks [R-AZ] and Congresswoman Yvette Clark [D-NY]); the Director of FERC's Office of Energy Infrastructure Security, Joe McClelland; state legislators involved in protecting the grid; retired General Officers of all four Services; retired Directors of relevant federal agencies;

24. David Perera, "Prospective Homeland Security Secretary Thad Allen Outlines Priorities in Senate Hearing," Fierce Homeland Security, September 11, 2013, http://www.fiercehomelandsecurity.com/story/prospective-homeland-security-secretary-thad-allen-outlines-priorities-sena/2013-09-11?utm_medium=nl&utm_source=internal (accessed September 18, 2013).
25. Paul Stockton, ASD (HS/ASAA), "Strategic Challenges for Warfare."
26. Foster, et al., *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures*, 158-171.

scientists and academics who have devoted their careers to this issue; and representatives from various academic critical infrastructure institutions.

MCCD personnel have been hands-on in promoting military and community protection and resilience. To this end, critical infrastructure vulnerability has been incorporated into cyber electives, workshops and wargames/exercises at CSLD. As an example, the Director of FERC's Office of Energy Infrastructure Security was a well-received guest speaker during the FY13 Cyber Elective.

CSLD sponsored workshops that have been conducted and are being planned include:

- In June 2010 a workshop, entitled "Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace,"[27] addressed catastrophic cyber attack, to include national security issues for preparation as well as response and recovery options for government organizations (especially military installations).
- A follow-on event was held in October 2010, in which CSLD hosted a 'first of its kind' workshop entitled "In the Dark: "Military Planning for a Catastrophic Critical Infrastructure Event,"[28] to explore the threats, vulnerabilities, and preparedness with respect to an electromagnetic pulse (EMP) attack or a direct hit by a CME.
- In October of 2011 MCCD personnel participated in a SECURE GRID tabletop exercise at the National Defense University.
- A "Cyber Futures Workshop" was held in 2012, which featured a "no cyber" scenario.[29]
- In March of 2013 CSLD conducted a wargame, in coordination with the Federal Reserve Board, to examine policy and strategic issues concerning government response to cyber hostilities.[30] It became clear that the effects of a cyber attack would rapidly spread to all CI/KR sectors, and have global impact.
- CSLD is presently preparing a workshop for early 2014 on authorities, rules of engagement, resiliency and COOP fundamentals as a result of an electric grid blackout due to robust cyber attacks.

MCCD is in the process of initiating a cyber course of instruction for Army senior leaders which will enhance their cyber situational awareness, inform them of cyber defensive and offensive fundamentals and interactions necessary for successful Unified Land Operations, increase awareness of skills and knowledge necessary to plan for and execute Mission Command in a degraded or denied space environment to continue operations in less than ideal conditions.

MCCD has representation in the following organizations:

- **The Task Force on National and Homeland Security** (sponsored by Congressman Franks through the Congressional EMP Caucus)
- **The EMP Coalition** (Honorable Newt Gingrich, Ambassador James Woolsey, co-chairs)
- **The Critical Infrastructure Defense Consortium** (working with Thomas Popik, Foundation for Resilient Societies, John Kappenman, Storm Analysis Consultants, and others)
- **InfraGard EMP Special Interest Group** (FBI-sponsored; Chuck Manto, Director)
- **The Center for Advanced Defense Studies** (working with LTC (Ret) Anthony Shaffer also in his capacity as a member of the Nuclear Strategy Forum)

MCCD personnel maintain close liaison with ARCYBER and CYBERCOM on varied cyber issues, providing support to wargames at both the USAWC and Fort Meade.

27. William Waddell, David Smith, James Shufelt, and Jeff Caton, *Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace* (CSL Study 1-11) (Carlisle, PA: U.S. Army War College, Center for Strategic Leadership, March 2011).
28. Kevin Cogan, *In The Dark: Military Planning for a Catastrophic Critical Infrastructure Event* (CSL Study 2-11) (Carlisle, PA: U.S. Army War College, Center for Strategic Leadership, May 2011).
29. William O. Waddell, James W. Shufelt, Jr., Jeffrey L. Caton, Kenneth D. Chrosniak, *Cyber futures Workshop Report* (CSLD Study 2-12), (Carlisle, PA: U.S. Army War College, Center for Strategic Leadership and Development, October 2012).
30. LTC Rob Purvis and COL Scott Forsythe, "Cyber Wargame Examines Policy and Strategic Issues," *The Torch*, Summer, 2013, http://www.carlisle.army.mil/banner/torch.pdf (accessed September 18, 2013), p 6.

Coordination with Fort Leavenworth Mission Command Center of Excellence (MCCoE) has been ongoing, as MCCD provided substantive Concepts Based Analysis (CBA) input and comments to analysts working on the Leadership, Doctrine, Education and Training team (LDE&T) Assessment. The focus of the assessment is to integrate robust cyber education and awareness in the senior-level officer educational curriculum. Additionally, MCCD is working closely with MCCoE's Degraded Space initiative in the Capabilities Development Integration Directorate to mitigate gaps associated with system vulnerabilities to environmental disruptions, threat interdictions, equipment or power generation failure and its affect on Unified Land Operations.

Several independent briefings have been provided by MCCD personnel to congressional representatives and their staffs on Capitol Hill. Threat testimony was given before the Maine State Legislature prior to the successful passage of their Grid Protection bill (the first State in the nation to do so). Numerous presentations have been provided to diverse audiences of first responders and emergency managers by MCCD personnel, who have also written extensively about critical infrastructure threat issues (published within a wide variety of venues as well as input provided to regulatory dockets on FERC rulemaking proposals).

THE WAY FORWARD

Retiring DHS Secretary Napolitano, speaking in front of the National Press Club, stated emphatically that a cyber attack on the energy critical infrastructure will change the picture of the United States, as it is a matter of not "if" but "when" we would lose electric power. She continued, saying that "our country will, at some point, face a major cyber event that will have a serious effect on our lives, our economy and the everyday functioning of our society." Secretary Napolitano further noted that "while we have built systems, protections and a framework to identify attacks and intrusions, share information with the private sector and across government, and develop plans and capabilities to mitigate the damage, more must be done, and quickly."[31] An economic collapse and severe civil unrest would surely follow a downed power grid, regardless of the cause for the massive outage.

The Secretary then stressed the importance of preparing for such an event, by supporting a viable and robust electrical grid system in the United States. This statement added credence to MCCD initiatives, and reinforced the fact that the Homeland is ill-prepared for a direct hit by a CME and/or a HEMP attack.

Still, concerns about a power grid breakdown are seldom discussed by citizens or the media. Nor do they appear to be planned for by the many entities involved in energy production and protection. The viability of the electric grid remains an issue and the threat is documented and credible. Natural and man-made events have the potential to place the lives of millions of Americans, as well as the sovereignty of our nation, in jeopardy.

31. Phil Mattingly, "Homeland Security Chief Says U.S. Should Expect 'Major' Cyber-Attack in Future," *Insurance Journal*, August 27, 2013, http://www.insurancejournal.com/news/national/2013/08/27/303108.htm (accessed September 16, 2013).

U.S. ARMY WAR COLLEGE
Center for Strategic Leadership and Development
650 Wright Avenue
Carlisle, PA 17103-5049

OFFICIAL BUSINESS

TERMINAL BLACKOUT:
CRITICAL ELECTRIC INFRASTRUCTURE VULNERABILITIES