THE MILITARY AUXILIARY RADIO SYSTEM (MARS):
A PARTNER IN THE NATION'S EMERGENCY PREPAREDNESS

Remarks by David J. Trachtenberg*
Before the Central Pennsylvania Chapter of InfraGard
Hershey, Pennsylvania
12 March 2014

[AS PREPARED FOR DELIVERY]

I would like to thank Dave Sherrid, Cindy Ayers, and the members of the Central Pennsylvania Chapter of InfraGard for the kind invitation to come and speak to you this morning. As a Pennsylvania native, I am always grateful for an opportunity to visit my birth state.

In preparing my remarks for today, I was reminded of the story of the breakfast speaker – an expert in cyber warfare – who became very agitated when informed by his host that he only had 15 minutes to speak. "Fifteen minutes?" he shouted, wagging his finger at the sponsor. "How do you expect me to tell this audience everything I know about this subject in 15 minutes?" To which his host replied, "Well, sir, I advise you to speak slowly."

As a policy practitioner, I don't pretend to be an expert in anything, so I will endeavor to follow that sound advice.

Having worked in government, I do know that no presentation can be taken seriously unless it is accompanied by PowerPoint slides. I despise what has been termed the "tyranny of PowerPoint." But at least the slides may provide a more interesting diversion than simply listening to the speaker.

As you know, I supported the work of the congressional EMP Commission. I also spent many years on Capitol Hill working policy issues for the House Armed Services Committee. In addition, I served as the Principal Deputy Assistant Secretary of Defense for International Security Policy in the George W. Bush administration, and as the Acting Deputy Assistant Secretary of Defense in the office responsible for nuclear weapons policy, missile defense, and related issues. And as a defense contractor, I oversaw my company's support to the Office of the Assistant Secretary of Defense for Homeland Defense in the area of Critical Infrastructure Protection.

My work in these areas reinforced for me the importance of maintaining the robustness and viability of our nation's critical infrastructures. I applaud your work – both independently and as members of InfraGard – to ensure the continued security and resilience of those infrastructures.

This is not an easy task. As Secretary of Homeland Security Jeh Johnson noted last month at the Woodrow Wilson Center, "the key to the government's efforts is to build trust with the

---

* David J. Trachtenberg is President and CEO of Shortwaver Consulting, LLC. He also serves as the National Planning Coordinator and Northeast Division Director for the U.S. Air Force Military Auxiliary Radio System (MARS).

private sector."[1] This organization is an excellent example of what a public-private partnership can do to help ensure our national security, and I thank you for your efforts.

I was asked to talk about a somewhat different kind of public-private partnership involving the communications sector – specifically, the Military Auxiliary Radio System (or "MARS") and the role it plays in providing a contingency communications capability to the Department of Defense (DoD), the US armed forces, and other government agencies.

So I'd like to do three things:

- First, briefly describe what MARS is and give a little bit of the background and history of this service;
- Second, explain how MARS fits into government plans to help ensure the functioning of the nation's critical communications infrastructure – it is an admittedly small role, but I think an interesting and perhaps unique one; and
- Finally, to provide some examples of how MARS has fulfilled its role during several emergency and disaster situations.

And of course I will leave time to answer whatever questions you might have about the program.

Let me begin with a question: Has anyone here heard of MARS? Usually when I tell someone I'm from MARS they say something like "Yeah, and I'm the Queen of England." But no, I'm not talking about the Red Planet.

MARS is a group of volunteer amateur radio operators, licensed by the Federal Communications Commission (FCC), who provide a backup communications capability to the government in the event that normal communications means are degraded, disrupted, or destroyed – either through natural disasters or deliberate hostile acts. Some MARS operators are current or retired military or civilian engineers, technicians, or communications specialists. Some are university professors and scientists, and some come from the defense industry.

MARS is a DoD-authorized and sponsored auxiliary organization, established by DoD Instruction, and is separately managed and operated by the Army, Navy-Marine Corps, and Air Force. I have been affiliated with the Air Force MARS program for more than 20 years, but all three MARS Services train, exercise, and work jointly.

Originally started in 1925 as the Army Amateur Radio System, operations were suspended during WWII and restarted in 1946 with participation of the Air Force. In 1962, the Navy and Marine Corps joined the program, which became the Military Affiliate Radio System.

Today, the program consists of roughly 5,000 radio operators who volunteer their time, services, and communications expertise – using their personal radio equipment and without

[1] Jeh Johnson, speech to the Wilson Center, 7 February 2014, accessible at http://www.wilsoncenter.org/event/conversation-secretary-homeland-security-jeh-johnson.

any compensation – to assist the Department of Defense and other federal, state, and local agencies with auxiliary communications in the event of a disaster or emergency… at no cost to the Government.

MARS operators receive specialized training and are additionally licensed by their respective military Service to transmit on frequencies set aside for their use by DoD using military protocols and procedures.

MARS is authorized and governed by DoD Instruction 4650.02, which establishes the purpose and mission of MARS. It also assigns responsibilities to various DoD entities for overseeing and integrating MARS into their operations. Policy oversight of MARS resides with the Deputy Chief Information Officer for Command, Control, Communications, and Computers and Information Infrastructure Capabilities (DCIO C4IIC) within the Office of the DoD CIO.

The primary MARS mission is to provide contingency radio communications support to U.S. Government operations. This includes support to the DoD and its Components, as well as to civil agencies at all levels, when requested. MARS also provides a means of allowing DoD civilians and contractors deployed in remote locations to send morale messages home – again, at no cost to the individual or the government.

In the past, before the days of cell phones, e-mail, Skype, and the Internet, MARS operators relayed morale message traffic over the radio between Service personnel stationed abroad and their families and friends at home. During Korea, Vietnam, and up through the first Gulf War in 1991, MARS operators passed thousands of messages from the troops overseas to their loved ones stateside. Some of you who served in the military may have even used MARS to send messages home from wherever you may have been stationed. Even today, MARS has been contacted by National Guard Family Readiness groups asking if we can still handle morale traffic for deployed troops on domestic operations such as Hurricane Katrina. The answer is yes.

Much has changed, however, as methods, procedures, and technology have advanced, and so has the mission of MARS.

Today, the main focus of MARS is emergency preparedness and disaster response. MARS support now includes providing auxiliary communications capabilities to DoD under the Defense Support of Civil Authorities (DSCA) framework. In addition, the Secretaries of the Military Departments, DoD Components, and Combatant Commands are authorized to make use of the backup communications capabilities that MARS provides and to integrate MARS into their activities. This has included Joint Service communications exercises, Continuity of Operations (COOP) and Continuity of Government (COG) planning, and other activities.

Most MARS communications take place in the high-frequency (HF) radio spectrum – what used to be called "shortwave radio" – using voice or digital communications modes. The Department of Homeland Security (DHS) "Communications Sector-Specific Plan," an annex to the National Infrastructure Protection Plan, classifies HF radio as part of the "wireless" communications infrastructure, noting that it "can be used for communication over great distances and between points separated by geographic barriers."[2] Using its organized

[2] http://www.dhs.gov/xlibrary/assets/nipp-ssp-communications-2010.pdf, p. 96.

networks of stations, MARS actually provides communications coverage at the state, regional, national, and international areas of operations.

Using HF radio frequencies, MARS operators even have the ability to send e-mail over radio through a distributed series of worldwide nodes to relay messages when Internet connectivity is unavailable. A number of civil agencies active in disaster response activities have the capability to pass message traffic and situational awareness reports to various recipients using this system, known as WinLink.

In cooperation with DHS, and working with the Federal Emergency Management Agency (FEMA), MARS participates in the National SHAred RESources (SHARES) HF Radio Program. SHARES is an interagency emergency message handling system that operates under the auspices of the DHS Office of Emergency Communications. It is intended to ensure national security and emergency preparedness communications in the event of natural or man-made disasters.

Like a fireman who hopes his services will never be needed, MARS members practice their communications skills on the air every day, training for an event they hope will never occur. But the reality of the world we live in is often not accommodating to our hopes.

So, MARS has a role to play as part of the U.S. Government's backup communications infrastructure – it is a small role, it is a modest role, but it is a valuable role when called upon in times of emergency.

Now, you may be wondering… why? Is this backup radio service really necessary?

After all, the U.S. military is the most formidable and technologically advanced military force in the world today. Our military superiority is unrivaled and our technological prowess virtually assures our dominance on the battlefield. The power of military communications technologies helps enable that superiority.

So why would the world's most powerful nation that employs sophisticated high-technology communications systems, including MILSATCOM assets and highly networked data and information capabilities, rely on a group of volunteer MARS operators using basic radio technology to facilitate the ability of its military to communicate?

It's a valid question – but I believe there is an equally valid answer.

With technological sophistication comes vulnerability – this is not only true for the communications sector, but other national critical infrastructures as well.

Our nation's increasing reliance on computerization, miniaturization, and sophisticated electronics provides tremendous benefits and enables the many conveniences of day-to-day living we enjoy in our society. But it also means that we are increasingly vulnerable to technological failures or countermeasures intended to degrade or defeat the very technologies on which we have become so dependent.

For example, you are all aware of the risk that electro-magnetic pulse (EMP) poses to our nation's critical infrastructures. Everything from power to transportation to food and water

distribution to emergency services to the banking and financial industry, as well as the communications infrastructure may be degraded or destroyed as a result of a natural or man-made EMP event.

For the communications sector, this means that many of the advanced capabilities the military relies on, from satellite terminals to other terrestrial communications links – especially those using commercial off-the-shelf technologies and electronics that are not hardened against EMP effects – may fail catastrophically… and all at once. Our critical national infrastructures are a system of systems, comprised of sub-systems, components, and nodes of varying degrees of vulnerability. As the saying goes, a chain is only as strong as its weakest link. And there are weak links in our national infrastructures, including our communications infrastructure.

Even under normal peacetime conditions, satellites fail or may not be available when needed. Other communications modes – from cell phones to the Internet – may also suffer outages or technological failures. In such times, the ability to rely on fundamental radio technology may be the difference between mission success and mission failure.

This is not to say that all radios are immune to EMP effects – they are not. But the newer, more technologically sophisticated radio equipment procured by the government is often more susceptible to EMP than many earlier models of radio equipment used by some MARS operators. Also, some MARS operators have taken special precautions to shield and protect their equipment to the extent possible from EMP effects.

Often times during natural disasters we hear or read stories of the local ham radio operator who provided an essential radio communications link when other communications means were unavailable. Sometimes, the only way to get information from Point A to Point B is via radio.

After the terrorist attacks of September 11, 2001, it was almost impossible for anyone in the Washington, DC area to make a phone call via landline or cell phone, as the regular phone line circuits were overwhelmed with the volume of callers. I was expecting to start work at the Pentagon shortly before 9/11, but bureaucratic delays postponed my transition from the Legislative to the Executive Branch. On that morning, hundreds of us were evacuated from the Capitol building and unable to contact anyone by phone. For hours (what seemed like an eternity), the only people I could communicate with were those standing next to me. My family had no idea if I was alive, and I didn't know if they were safe.

More recently, after Hurricane Sandy that pounded the East Coast in October 2012, large areas of NY and NJ were without power and communications for extended periods of time.

In these types of conditions, radio is an effective means of relaying messages and conveying situational awareness to public authorities and first responders. The combination of HF and VHF radio can provide local, regional, and long-distance communications – which may be essential in a crisis or emergency that affects a wide geographical area.

Then, of course, there is also the possibility that communications can be deliberately disrupted as a result of hostile action. We know that asymmetrical warfare against the United States may include kinetic, directed energy, and cyber attacks against our

communications infrastructure, including military and civilian communications satellites and the ground-based systems used to deliver essential information.

Last April, for example, fiber-optic telecommunications cables were cut in what is considered to have been a deliberate assault on a power substation near San Jose, California. As *The Wall Street Journal* reported, the cables were cut "in a way that made them hard to repair," raising concerns over the prospect of deliberate terrorist action that could drop the power grid or communications infrastructure for an extended period of time.[3]

The crisis in Ukraine provides a contemporary example. At the start of the crisis, *The New York Times* reported:

> "Mobile, landline and Internet access has been cut off in parts of the Crimea region, according to a statement from Ukrtelecom, the Ukrainian National Telecommunications operator. The company said…that 'unknown people seized several communications hubs in Crimea' and damaged fiber-optic cable belonging to the company. As a result, the company said it had 'lost the technical capacity to provide connection between the peninsula and the rest of Ukraine and probably across the peninsula, too.' Ukrtelecom added that 'communications services are vital to sustain essential support systems in the peninsula including first aid, fire and rescue services.'"[4]

Now while this particular outage reportedly lasted for only several hours, it demonstrates once again the susceptibility of normal communications infrastructures to deliberate sabotage or intentional disruption.

Imagine for a moment the implications if, as a result of deliberate action, the state of Pennsylvania was cut off from landlines, cell phone availability, and Internet access. (My daughter freaks out when she loses WiFi service or can't find a "Hot Spot.")

Here in Pennsylvania, the state's Emergency Management Agency (PEMA) became a model for the nation in adopting an Emergency Management Network using satellite-based assets and an Emergency Alert System to distribute audio and text messages statewide. According to PEMA, this "provides us the ability to communicate during emergencies where Emergency Activations are necessary."[5]

Unfortunately, there are multiple ways the normal means of communication on which we heavily rely can be degraded. These can range from physical attacks on infrastructure to cyber attacks that could cripple the network. The Federal Communications Commission has reported that "The number of incidents of documented attacks on computer-based systems

---

[3] http://online.wsj.com/news/articles/SB10001424052702304851104579359141941621778, 18 February 2014.

[4] http://thelede.blogs.nytimes.com/2014/02/28/latest-updates-tensions-in-ukraine/?action=click&module=Search&region=searchResults%230&version=&url=http%3A%2F%2Fquery.nytimes.com%2Fsearch%2Fsitesearch%2F%3Faction%3Dclick%26region%3DMasthead%26pgtype%3DHomepage%26module%3DSearchSubmit%26contentCollection%3DHomepage%26t%3Dqry45%23%2Fukrtelecom, 28 February 2014.

[5] http://www.pema.state.pa.us/portal/server.pt/community/programs_and_services/4547/warning___communications_systems/458191.

and communications systems increases on a daily basis."[6] And many of these threats emanate from overseas. Iran, for example, has asserted that its capture of an unmanned U.S. Sentinel drone in 2011 was enabled by Iranian electronic warfare specialists who managed to sever the U.S. military's communications links to it.[7]

So the answer to the question "Why MARS?" is that as a backup, auxiliary means of communication – especially in today's heavily computerized, digitized, and technology-dependent society – it makes sense.

So how has MARS exercised its role? Let me give you a few examples.

The Army-run component of MARS is headquartered at the Army's Network Enterprise Technology Command, or NETCOM, at Fort Huachuca, Arizona. Army MARS maintains a network of overseas stations where U.S. forces are deployed and has had HF radio operators in places like Iraq and Afghanistan capable of communicating stateside.

Last month, Army MARS members trained soldiers from the Illinois National Guard in a variety of HF radio techniques, including propagation and antenna analysis. The soldiers then participated in an exercise where they made radio contact with various MARS operators throughout the Midwest.

In January, several Army MARS teams deployed to support a Texas State Guard Regimental training exercise at two locations in Texas, where they established contact with the Guard headquarters in Austin. In support of the exercise, the MARS operators successfully relayed a series of military messages using various digital communication modes.

MARS participation in these types of exercises is increasingly common and demonstrates a strengthening of the relationship between the National Guard and MARS.

Navy-Marine Corps MARS, which is headquartered in Williamsburg, Virginia, has been working with hundreds of civil agencies and emergency response organizations to ensure MARS can interoperate with them in the event of emergencies. This includes use of the WinLink "e-mail over radio" system and other digital modes of communications.

At the federal level, Navy-Marine Corps MARS operators helped set up the SHARES HF "radio-only" traffic system using WinLink. Between 1,000 and 2,000 messages are relayed each month using this system, which has demonstrated the practical ability to send e-mail traffic in the absence of Internet connectivity.

And Air Force MARS, with its headquarters at the 38th Cyberspace Squadron at Scott AFB, Illinois, provides daily support to active military aircrews flying operational missions worldwide. Among its other activities, Air Force MARS operators run a Phone Patch Net on a 24/7 basis, providing cost-free phone patch capabilities to pilots and flight crews seeking to contact military and civilian ground stations. These patches link aircraft with ground stations

---

[6] http://www.fcc.gov/help/public-safety-tech-topic-20-cyber-security-and-communications.

[7] Jason Mick, "Iran: Yes, We Hacked the U.S.'s Drone, and Here's How We Did It," *Daily Tech* blog, accessible at http://www.dailytech.com/Iran+Yes+We+Hacked+the+USs+Drone+and+Heres+How+We+Did+It/article23533.htm.

through a regular telephone connection and can be for official business or simply morale phone calls to family members.

Let me mention a few examples of how the Phone Patch Net assists military aircraft on a daily basis.

A few weeks ago, a U-2 aircraft flying outside the continental United States contacted the Phone Patch Net on its primary HF frequency requesting several telephone patches as a result of warning lights coming on and aircraft systems shutting down. The pilot made a call for assistance and our operators responded by patching the pilot through to his base command post, operations center, and other locations, where he received instructions on what to do and where to land.

The following week, a C-17 over the North Atlantic lost cabin pressure and had to make an emergency landing. The communications for this were provided by the Phone Patch Net.

Let me give you one more example. A while back, a civilian airliner carrying hundreds of passengers over South America encountered severe weather that affected the plane's instrumentation and jeopardized its ability to continue safely en route to its destination. The pilot – a former Air Force officer – used an on-board HF radio to contact the Phone Patch Net for assistance. The MARS operators were able to connect the pilot to the Operations Center of a destination airfield for instructions, allowing the airliner to land safely.

While you won't hear or read about incidents like this, such calls are more common than you might imagine.

This information isn't classified. After all, the phone conversations are transmitted "in the clear" over unencrypted HF radio frequencies – meaning anyone with a shortwave radio and sideband reception can monitor these phone patches. The equipment needed to monitor these transmissions is no more sophisticated than this Sony shortwave radio receiver that fits in my shirt pocket.

Each year, Air Force MARS Phone Patch Net operators conduct more than 2,000 phone patches for military aircraft – most of which are related to ongoing mission operations. Importantly, the military's use of the MARS network frees up more sophisticated and costly military communications assets for other purposes – and in today's austere budget environment with the challenges of sequestration, this is a net plus.

Let me cite some other examples of how MARS operators support the nation's communications needs.

During National Security Special Events, MARS stations establish continuous on-the-air liaison with the FEMA National Emergency Coordination Net, SHARES network, and military and other communications centers to disseminate information and pass emergency traffic as needed.

The MARS communications station at the Pentagon provides contingency communications to the Joint Staff and the National Military Command Center (NMCC) and participates in communications exercises with DoD airborne assets. Encrypted off-line messages from

airborne assets are sent through the Pentagon MARS Station, where they are passed to the NMCC for decryption.

During "Superstorm Sandy" in 2012, MARS facilitated communications for National Guard units conducting disaster relief and search and rescue operations, as well as responding to medical emergencies, in a wide area of the northeast United States. Specifically, MARS operators provided emergency communications linking the command posts of several responding organizations to their deployed response units on Long Island and in Brooklyn; facilitated the coordination of cargo manifests for transport of emergency equipment into the affected areas; supported HF and VHF communications during ground Search and Rescue operations; trained emergency responders on the use of the Air Force MARS Phone Patch Net when their landline telephone, cell phone, texting, Internet e-mail, and DSN telephone services were severed; assisted with on-the-air HF radio communications training and testing for multiple responding agencies; and handled safety-of-flight radio traffic regarding hazards caused by the storm.

So MARS enjoys an active partnership with the military – Active, Reserve, and Guard – as well as other Federal and State agencies and Emergency Operations Centers.

MARS has also played a modest role in responding to overseas disasters. For example, in response to the 2010 earthquake, volunteer MARS operators deployed to Haiti to provide communications support to the military, and to medical and humanitarian organizations. Their deployment was not the result of an official MARS activation – rather they traveled under the auspices of the non-governmental organizations they supported. But these Army, Navy-Marine Corps, and Air Force MARS operators received approval from their respective Chiefs to utilize the full resources of MARS for their operations, which saved lives.

Working with established MARS networks, amateur radio operators along the East and Gulf coasts, and doctors from the University of Miami Medical Center's Project Medishare, MARS operators helped to coordinate communications among military units and between military units and non-governmental organizations (NGOs), and coordinated military helicopter MEDEVAC and sealift of injured residents to the USNS Comfort, which was stationed off the Haitian coast. This was the first significant use of joint MARS assets in response to a major overseas disaster in which almost 300,000 people were killed and a country's infrastructure collapsed.

More recently, MARS was tasked by DoD to assist as required in the military's humanitarian response efforts after Typhoon Haiyan struck the Philippines last year.

Now I don't want to oversell the capabilities of MARS or its importance. The laws of physics are immutable, and even HF radio suffers from limitations caused by solar storms and other geomagnetic disturbances that can play havoc with long-distance propagation. As an Army MARS manual on EMP published last December explained, "HF radio is more susceptible to disrupting effects of nuclear explosions in the atmosphere than is any other frequency band. This is primarily due to catastrophic changes in the ionosphere. Such changes occur rapidly after the explosion and last for several minutes to several days."[8]

[8] Department of the Army, Military Auxiliary Radio System, AM 5-602, *Electromagnetic Pulse (EMP)*, December 2013, p. 4-1, accessible at

While we can't do anything about the ionosphere, there are steps that can be taken to protect radio equipment from the debilitating effects of EMP. Moreover, the ionosphere typically recovers from a solar flare or coronal mass ejection and similar conditions created by an EMP faster than it takes to replace critical military and civilian communications satellites and infrastructure.

MARS is a diverse organization, and not all MARS members are actively engaged in the kinds of activities I have talked about here. But although they come from multiple backgrounds and all walks of life, they are united in their spirit of volunteerism and desire for public service. Above all, MARS is an organization of men and women who enjoy the technical challenge of communicating over the airwaves.

As a former Secretary of the Air Force told me several years ago, "It's a great thing that Americans from so many walks of life take their free time, or hobby, and turn it into something useful for our country and those in need."

In many respects, I believe MARS reflects the same principles of public-private partnership that guide InfraGard's activities.

In closing, I'd like you to remember these three main points:

- The United States maintains the most sophisticated Command, Control, and Communications system in the world;
- With increased sophistication comes increased vulnerability;
- One of the responses to the identified vulnerabilities in communications systems is the work of the Military Auxiliary Radio System – a system that has provided this volunteer service to our country for nearly 90 years.

I appreciate your time, your hospitality, and most of all your continuing efforts to help safeguard the critical infrastructures on which our nation's security and well-being depends.

I would be glad to take any questions.

[END PREPARED REMARKS]

---

https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxhcm15bWFyc3BvcnRhbHxneDoxMDc1ZGY1MjljZmU4NGRj.