Commander, U.S. Pacific Fleet
AFCEA TechNet
Honolulu, Hawaii
Admiral Harry B. Harris Jr.
05 December 2013
As prepared for delivery

Thanks, Marc, for that great introduction.

Admiral Macke...Secretary Grimes...DONCIO Halvorsen...AFCEA President Schneider... AFCEA Hawaii Team…General Wood…And a special shout-out to the ROTC and JROTC cadets. I started out a hundred years ago as a NJROTC cadet in high school.

Ladies and gentlemen – good morning. It's wonderful to be with you today and see so many friends from my N6 days and from AFCEA gatherings literally all over the world.

Folks, my job is to do the speaking...and your job is to do the listening. So let's make a deal…if you finish your job before I finish mine, just let me know and we'll wrap this up wiki-wiki.

Now for all you tech junkies that think that I just made a bad joke about a web application, wiki-wiki means "very fast" in Hawaiian. So if you learn nothing else from me today, you've got that to impress your friends.

For those who have read my bio, and have not yet left the room, you know my career has centered around operations. But just a few years ago I was assigned as the deputy CNO for communication networks, "OPNAV N6," which made this analog throwback the Navy's top "computer guy." Talk about a fish out of water. So I had to get smart on all this IT and cyber stuff like, well, wiki-wiki.

I would have been completely lost were it not for folks like Archie Clemins, Dick Macke, Denby Starling, Barry McCullough, Bob Stephenson, Terry Halvorsen, Diane Webber, Nancy Norton, Jerry Tuttle, Jerry Flowers, the late Gary Federici, and the pros from AFCEA, to name a few.

Now, in my current job, I find I'm focused on both fleet operations and fleet networks. So my time as N6, struggle though it was for me, in fact made me a better fleet commander. Certainly it's made Linda Newton's job a little more challenging.

And here I am speaking at TechNet on "Building Coalitions Through Cyber." This is an important topic and one I am excited to talk about.

As this audience knows well, today's world is interconnected and interdependent in ways unimaginable only a generation ago. Today, not only does 90 percent of the world's commerce travel by sea, but 95 percent of all Internet traffic travels under it. To maintain security and stability which underpin economic prosperity in the Pacific, and America is a Pacific nation, where we all rely on the seas for movement of commodities and information, we must ensure that free and unfettered access to the maritime domain is guaranteed to all. For America, that

responsibility often falls to your Navy writ large, and out here, to the Pacific Fleet. For over seven decades, we've maintained a continuous and robust presence in the Western Pacific. Now, as the U.S. continues our rebalance to the Indo-Asia-Pacific, I can assure you that the Pacific Fleet will remain a credible and capable force.

Of course, we also focus on the Indian Ocean. I like to say we operate from Hollywood to Bollywood, and from polar bears to penguins.

Now, most of the 52 percent of the globe that's our area of responsibility is the vast open ocean, which makes reliable secure communications an operational imperative.

But we're not just trying to improve those capabilities that already exist today. We are looking to our partners in industry to develop new technologies and cutting-edge capabilities so that we can assure our ability to command and control in challenging environments. We depend on the capabilities that you provide to ensure we deliver decision superiority. That is, knowledge, information, intelligence, data and orders to the warfighter, and back, virtually, instantaneously, against 21st century cyber threats, and do it in a fiscally constrained environment. That last part is especially relevant today, so let me say that again -- a fiscally constrained environment.

Back when I was N6 I knew we couldn't afford to invest in every IT good idea that industry had to offer. Then, as now, we have to be judicious with every dollar we spend. We simply can't afford to invest in single-mission systems and single-mission platforms, we've got to focus on multi-mission systems and platforms to enable us to do what we do more effectively, in less time, and with fewer operators.

Now I'm not a big acronym guy, but in the Navy we seem to have one for everything. Especially in your world. Because the 52 percent of the globe that the Pacific Fleet operates in is open ocean, we are forced to be prepared to operate in a DIL -- D-I-L -- environment. Disconnected / Intermittent / Low Bandwidth. It's a funny little acronym if you ask me, and as someone from my N6 department recently pointed out, in a DIL environment we would also have Restricted Transmissions. So that would make the acronym DILBERT. See why I don't like acronyms? You just never know where to stop.

Anyway, DIL is a challenge even on a good day, especially in the maritime domain, where we might operate thousands of miles from any large land-based network. We have to rely on satellite communications, and sometimes even a simple glitch in the system can cause us some pretty big problems. Not to mention the challenges we would face in an adversary-induced DIL environment.

Today we're looking to shore up our vulnerabilities in a DIL environment by working to develop what we call the C2 Thin Line, those absolutely critical command and control services that are required to allow us to fight in a comms-degraded environment. Or through a cyber-attack.

After years of working to increase our bandwidth, we now realize we're going to have to learn, or maybe I should say "relearn," to operate and fight with less bandwidth when we are denied our full capacity. This is more than a technical challenge. We must change our doctrine and tactics

to fit this new reality. As you build the tools and equipment we need to fight and win, they have to work in a DIL environment. Or I will simply recommend that we buy something else that does.

But it is not only your Navy and sister services that must learn to work in DIL environments, so too must non-governmental organizations, partners and friends throughout the region, especially for complex humanitarian assistance and disaster relief operations. We must improve our ability to communicate with them, especially when they are the supported agencies and we are the supporting forces.

PACFLT works with our allies and partners to advance our maritime relationships, improve information sharing, and enhance cyber security…and of course…working with them to improve our effectiveness in a DIL environment. We do this through exercises like Cooperation Afloat Readiness and Training, or CARAT, Malabar, AnnualEx, Cobra Gold, and so on. Consider the Rim of the Pacific exercise or RIMPAC, the largest maritime exercise in the world. RIMPAC 2014 will involve 23 countries, including for the first time, China. These exercises tell me that we must be able to conduct cross-domain chat between participants to overcome the challenge of communicating at various classification levels. That's where you come in. I wouldn't know a wham-a-dyne from a rock 'n' roll band. But you do and I'm counting on you to build it for me.

Our access to information has increased our ability to execute our missions, across a complex tactical, operational, and strategic landscape, but it also presents vulnerabilities and opportunities to our adversaries. In the news, we are seeing increasing reports of cyber-attack activity from "hacktivists" and nation states looking for shortcuts to advance their technological ambitions. By adversaries who simply cannot compete against our traditional military forces -- in fact, why would they? -- by adversaries who are unconstrained by law, regulation and policy, by adversaries who view cyber intrusions, exfiltrations and attack as their new normal.

By adversaries who view these activities as simply asymmetric means to exploit any weaknesses we may have. We simply cannot afford to let this continue. Former Secretary of Defense Panetta warned, and I quote ". . . it is very possible our next Pearl Harbor could be a cyber-attack . . ." A sober warning here in Hawaii that can't be ignored.

Today we are working with the U.S. Pacific Command to extend legal relationships with partner nations to improve cyber security for us, as well as them. Just two weeks ago, our SecDef directed that all new DOD contracts must meet minimum specifications for cyber security. This direction requires defense contractors to protect the unclassified, but sensitive, information on their networks. This unclassified information could be a treasure trove of data that directly benefits our adversaries by giving them better understanding of our systems, insight into our day-to-day operations, and leveraging our technology without the costly research and development investments that we've all made. I believe this new policy will not only protect our industry partners' intellectual capital, it will also ensure we maintain the technological advantage we need to operate forward, and fight and win, whether that's high-end air-sea battle or disaster relief operations.

Now let me talk about some of the exciting new technologies coming online. First, there is CANES, yep, another acronym. Consolidated Afloat Network and Enterprise Services. It's the

Navy's next-generation tactical afloat network which consolidates legacy networks into a single integrated platform with increased capability for defense and security. It serves as the single cyber platform for more than 200 applications and connected systems, many of which can now be moved into a virtual environment. CANES will greatly standardize our afloat network configuration, and I believe CANES will drive cost savings and reduce cycle times for maintenance, applications and modernization.

As OPNAV N6, I worked hard to get CANES to the fleet. That was three jobs ago. Truthfully, I never dreamed I would get to actually touch CANES. Well, two weeks ago, I had the opportunity to visit USS Chafee, one of our guided-missile destroyers, right here on the waterfront. While onboard I got to see and touch CANES. The CO of that ship must have thought I was crazy; he just couldn't understand how I could be so excited about seeing those boxes getting installed. For me, that was a really good day.

But CANES is only part of the good news story. The fleet is starting to realize benefits of other modernization efforts. The Navy Multi-Band Terminal, NMT, allows our ships to more effectively use new-capability military SATCOM services with a single integrated terminal, instead of multiple terminals. ADNS Increment III – or Automated Digital Networking Services – gives us the ability to use all SATCOM services through automation with increased security to support multiple missions like anti-air warfare, anti-surface warfare, anti-submarine warfare, air and missile defense. These programs are force multipliers.

Today we're also implementing something called the Joint Information Environment, or JIE. The JIE aims to provide out warfighter and mission partners with a shared IT infrastructure and a common set of enterprise services all under a single security architecture. It consists of networked operations centers, core data centers, and a global identity management system with cloud applications and services.

I spoke about JIE to an AFCEA gathering in 2012. I'm a believer and I saw it work in my last job on the Joint Staff. JIE will improve integration of information technologies and operations, while increasing our ability to respond to security breaches across our own networks. JIE will provide the overall framework and common standards to help address the challenge we face, not only for joint US forces, but the mission partner environment, like non-governmental organizations and the State Department, which we closely work with during humanitarian assistance and disaster relief efforts, like the one recently conducted in the Philippines, Operation Damayan. JIE will be an interoperable network architecture that operates across multiple security domains for all mission partners, with increased security, effectiveness, and efficiency.

PACOM has already been approved to lead JIE Increment 2 in the Pacific. Why? Well, first, improved mission effectiveness and operational flexibility. This means agile information systems that enable C2, for all PACOM missions, and any set of PACOM partners. It means resilience in "DIL" environments. The benefit will be improved readiness by adding agility to C4 infrastructure. We need to embrace JIE, or be left behind.

Second, there's a need for increased cyber security. We require robust information systems that provide the integrity, availability and confidentiality needed to assure C2 for all PACOM

missions and any set of PACOM partners in all security domains. The benefit here will be improved cyber security through rapid use of the latest protocols, standards and best practices. The operative word here being "rapid."

Finally, we need improved IT efficiencies and joint information services. Interoperable information systems developed and implemented with maximum performance, reliability and expandability at the best value with minimum waste. We will see decreased costs by adopting common universal C4 infrastructure and practices for all network enclaves.

Now, I've spoken for about 15 minutes already, probably not as wiki-wiki as some of you would have liked. Recently, on a trip to Australia, I was the last speaker in a long lineup that went through dinner. Afterwards, as we were getting ready to leave, one of the ladies there said to me, "Admiral, I really enjoyed your speech. I woke up so refreshed."

I'm glad to see so many of you are still awake, maybe you just woke up refreshed.

Ladies and gentlemen, since I'm the last person between you and Waikiki, let me close with this thought.

The United States Navy is second to none. We evolve and adapt better than anyone in the world. That's not based on reading about it, that's based on operational experience, and that comes from a synergy between our nation's brave sons and daughters who have chosen the warrior way, and the people and organizations in industry that provide the best equipment and technology that enables them to get the job done. Our strength comes from leaders in industry who are well aware of the challenges, opportunities and dangers we face around the world, and the young men and women who wear the cloth of the nation, who run toward, not away, from the sound of the guns.

I truly thank you for all you do on a daily basis to help ensure our military and our nation remain ready to fight tonight.

May God bless our men and women who serve on the forward edge of the battle area – the FEBA of freedom – at sea, in the air, in Afghanistan and the far reaches of the Pacific.

May God bless the veterans who stood tall here in Hawaii in the closing days of 1941.

And may God bless this land of liberty we call America.

Thank you.