COMBINED ENDEAVOR

U.S. EUCOM C4/CYBER EXERCISE ENHANCES INTEROPERABILITY

By Robert L. Watson
Chief of the Combined Interoperability Branch, U.S. European Command

Photos by EUCOM

IN 2014, the United States European Command (EUCOM) celebrates the 20-year anniversary of Combined Endeavor, the premier interoperability and cyber defense exercise between NATO and Partnership for Peace (PfP) nations. In September 2013, more than 1,200 people from 40 nations and transnational organizations gathered in Grafenwöhr, Germany, to test their interoperability and cyber defense skills in a collaborative environment.

During the past two decades, this exercise has become the bellwether of interoperability training for NATO and PfP nations and now has become so for cyber security as well. It began with 10 countries seeking to achieve multiple layers of interoperability at the technical and systems level and,

Participants from 40 nations take part in Combined Endeavor 2013 in Grafenwöhr, Germany.

even more importantly, at the human level. The U.S. Department of Defense defines interoperability as "the ability of systems, units, or forces to provide data, information, material and services to and accept the same from other systems, units, or forces, and to use the data, information, material, and services exchanged to enable them to operate effectively together."[1] Combined Endeavor began with this premise.

The exercise has changed so much during the past 20 years it is barely recognizable. The learning experience leverages the collective knowledge available only in an environment of this sort. The Cyber Operations Center and Cyber Defense Seminars by leading industry experts, not to mention a Combined Joint Command and Control Center, are some of the highlights of this unique exercise. At Combined Endeavor 2013, an exercise network similar to that of the International Security Assistance Force (ISAF) in Afghanistan was built within two weeks. Although the interoperability and cyber security skills experienced in this exercise cannot be replicated, other major U.S. commands have used Combined Endeavor as a model to build similar exercises with different partners.

Sustaining the interoperability and cyber defense gains from the past 20 years will not be easy, given the challenge of austerity in manpower and financial resources. Budgets are tight, and 2014 looks to be a difficult year for fiscal stability on the heels of the global financial crisis. In 2013, the U.S. experienced a partial government shutdown and widespread budget cuts. In Europe, crushing debt issues have burdened Greece, Iceland, Ireland, Italy, Portugal and Spain.[2] While opportunities for fruitful collaboration may seem great, opportunities may also be fleeting.

Slovenian soldiers operate information systems during Combined Endeavor in Grafenwöhr, Germany.

TRANS-ATLANTIC AUSTERITY

NATO projects that defense budgetary spending will continue to contract. Most NATO nations will not come close to the Alliance's 2-percent-of-GDP target for defense spending in 2014, nor probably in the near future.[3] Even the U.S. is feeling the pressure. The 2013 Budget Control Act mandates billions of dollars in spending cuts during the next five years and reduces manpower to levels not seen in 20 years. With these budgetary pressures, maintaining interoperability within NATO and with coalition partners will be increasingly difficult.

This is significant because the threats from nontraditional vectors, such as cyber, continue to increase rapidly. Many lessons in interoperability are born of a collective desire to improve the ability to share information seamlessly and transparently. During the past 20 years, there have been remarkable gains in interoperability and partnerships. The ISAF coalition is a shining example of the ability to forge interoperability in spite of austerity.

REFLECTION ON OPPORTUNITIES

Within the context of austerity, it is important to understand the great opportunities that the past two decades have provided from both a European and a trans-Atlantic perspective. U.S. President Bill Clinton's 1994 United Nations address provided foreshadowing: "Our struggle today, in a world more high-tech, more fast-moving, more chaotically diverse than ever, is the age-old fight between hope and fear."[4] In 1994, the peace dividend of the Cold War proved substantive as the U.S and Russia signed the Kremlin accords, effectively ending the intentional aiming of nuclear missiles at each other and providing for the dismantling of the nuclear arsenal in Ukraine.[5] That same year, Finland and Sweden decided to join the European Union, and the Russian Army completed its withdrawal from Estonia and Latvia.[6] Meanwhile, in the Pacific, China connected to the Internet for the first time.[7] Unfortunately, the Balkan wars were still raging following the breakup of Yugoslavia.

In January 1994, NATO launched PfP to aid countries seeking cooperative military and peacekeeping relations with the Alliance. On July 7, 1994, in Warsaw, Poland, President Clinton announced an American commitment to provide assistance to new democratic countries in line with PfP goals. This led to the creation of the Warsaw Initiative Program, managed by the U.S. departments of

State and Defense to improve relations and military interoperability between NATO and countries committed to democratic principles.[8] The Warsaw Initiative Fund paved the way for generations of partnerships by enabling developing countries to participate in opportunities such as Combined Endeavor and a host of other creative and innovative programs to achieve mutual defense goals.

WHAT A DIFFERENCE 20 YEARS CAN MAKE

Twenty years later, it is difficult to remember how much harder it was to share information among coalition members. Radios have been eclipsed by lightning quick, accurate data communications across multiple domains. Combined Endeavor 2013 highlighted several notable firsts in interoperability resulting from many years of effort and risk-taking. For example, the French Army successfully fired artillery using a U.S. fire support system.

This also marked the first year of a persistent and consistent approach to improving collective cyber security capabilities. An entire cyber security cell was established to test the network's strength on multiple fronts. In the 2012 Joint Operational Access Concept, Adm. Michael Mullen, then chairman of the U.S. Joint Chiefs of Staff, described core military competencies necessary for successful operations: "complementary multi-domain power projection" and the "ability to maintain joint assured access to the global commons and cyberspace should they become contested."[9]

Indeed, some European nations, such as Georgia and Estonia, have experienced firsthand aggression in cyberspace. Cyber Endeavor addresses the complexities of the cyber domain and focuses on it, not just in the capstone exercise at Grafenwöhr, but also through successful regional cyber security seminars across Europe. The seminars aim to take advantage of gaps in capabilities and capacities and improve the collective cyber security posture of key partners in Europe.

A COLLABORATIVE APPROACH

Patience and perseverance are required to ensure interoperability gains are not lost. Understandably, no single nation can solve every dilemma and resources are finite, but, opportunities for collaboration must be seized in spite of austerity. U.S. Army Europe's Joint Multinational Readiness Center hosts an exceptional facility at Grafenwöhr that has taken this collaborative approach to high levels in mission rehearsal exercises for European partners. Other notable examples are the Cooperative Cyber Defence Centre of Excellence in Estonia and the Command and Control Centre of Excellence in the Netherlands. NATO and partner nations must continue to take every opportunity to exercise and maintain interoperability. It is critical to capitalize on these efforts, to expand upon the lessons learned and solidify interoperability between partner nations.

ASSURED ACCESS

It is imperative that interoperability provide assured access to information and data. Only through assured access can national leadership attain strategic flexibility. Interoperability solutions must be tested, tailored and scaled to meet operational requirements. More importantly, they must be synchronized across multidomain requirements of command and control, cyber and spectrum. Combined Endeavor provides an excellent venue to test solutions in all these domains. Assured access mandates an ability to provide defense in depth. Mutual trans-Atlantic interests have been firmly cemented in the past 20 years, and Allied cooperation has never been more important. Intersecting national interests create opportunities to strengthen mutual defense goals and objectives, as well as to develop common strategies to achieve goals that might be unattainable unilaterally.

The role of defense in cyber security cannot be overstated. In 2009, Cyber Endeavor was created to build the cyber defense capability of partner nations, and compliment Combined Endeavor. In recent years, the growth of Cyber Endeavor, in concert with Combined Endeavor, has been impressive because almost every Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) system has some network capabilities. Cyber Endeavor provides EUCOM and coalition partners an invaluable opportunity to collaborate on cyber defense issues and build cyber defense partnerships with NATO, partner nations, academia and industry. Subsequently, the goal is to strengthen the collective international cyber defense posture and to improve force readiness for deployment with secure C4ISR systems in support of multinational crisis response.

Finally, a collaborative approach to interoperability and cyber security is imperative to address risks and vulnerabilities that will only increase. Over the next year Combined Endeavor will evolve from using a centralized approach to a decentralized approach. Specifically, EUCOM will integrate the Mission Partner Environment and cyber security threads into the Command's Regional Exercise Portfolio. It is therefore imperative that complacency is avoided and interoperability is fostered at every opportunity. Decision-makers and leaders must not allow difficult situations and austerity to drive defense readiness, especially in the communications and cyber domain. □

1. Chairman of the Joint Chiefs of Staff Instruction 6212.01F, March 21, 2012, p. 49, http://jitc.fhu.disa.mil/jitc_dri/pdfs/cjcsi_6212_01f.pdf
2. "The Eurozone in Crisis," Council on Foreign Relations, Cristopher Alessi, April 3, 2013, http://www.cfr.org/world/eurozone-crisis/p22055
3. "NATO and The Challenges of Austerity," F. Stephen Larrabee et al, Rand Corp., 2012, http://www.rand.org/pubs/monographs/MG1196.html#key-findings
4. Address by President Bill Clinton to the 49th UN General Assembly, September 24, 1994, http://www.state.gov/p/io/potusunga/207377.htm
5. "In Disarmament Breakthroughs, Clinton, Yeltsin Sign Nuclear Accords," Terrence Hunt, AP News Archive, January 14, 1994, http://www.apnewsarchive.com/1994/In-Disarmament-Breakthroughs-Clinton-Yeltsin-Sign-Nuclear-Accords/id-c47d24f57ae53350868e17ea094a17e0
6. "Anniversary of the Withdrawal of Russian Troops from Estonia," http://estonia.eu/about-estonia/history/withdrawal-of-russian-troops-from-estonia.html
7. "China Celebrates 10 Years of Being Connected to the Internet," Stephen Lawson, 17 May 2004, http://www.pcworld.idg.com.au/article/128099/china_celebrates_10_years_being_connected_internet/
8. U.S. Assistance to the Partnership for Peace, US GAO, July 2001, Washington, D.C., http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-01-734/pdf/GAOREPORTS-GAO-01-734.pdf
9. Joint Operational Access Concept, DoD, Version 1.0, Washington, D.C. January 17, 2012, http://www.defense.gov/pubs/pdfs/joac_Jan%202012_signed.pdf