

AFCEA Welcome/Opening Keynote Speech

**Murad Bayar, Undersecretary for Defense Industries,
MoND, Turkey**

A Turkish Perspective on the Challenges of Security in a Network-Enabled Environment

I would like to begin my address by welcoming everybody to Turkey and Istanbul on the occasion of the AFCEA – Technet Europe 2010 Symposium. It gives us great pleasure to host this event focusing on connectivity, which is in fact a historical characteristic of Istanbul in connecting two continents.

I believe that this symposium focusing on the challenges of developing network-enabled capabilities while managing security implications will serve AFCEA's mission of increasing knowledge in information technology and communications.

Undersecretariat for Defense Industries (SSM) is the main procurement agency for armament requirements in Turkey. We are also responsible for the development of Turkey's national defense industry. Our industry goals are specified in SSM strategic plan and individual sector strategies which includes the C4I sector. Information technologies constitute one of our key priority areas as a force multiplier.

In managing defense procurement programs, interoperability with NATO and other allies is a key criterion. While simply purchasing other countries' equipment would provide interoperability, that equipment might not suit Turkish Armed Forces' unique military requirements. Consequently, SSM turns to Turkish defense industry to provide it with customized solutions with state of the art technologies.

Cyber warfare has become a major concern for the governments, militaries and civil agencies over the last decade. Technical publications about information security increased more than four-fold during the first decade of the 21st century. Financial loss has reached to 1 trillion \$ due to cyber attacks by the end of 2008. Online bank customers in the US lost more than half a billion dollars to Internet thieves in 2009 according to statistics from the Internet Crime Complaint Center, which is more

than twice the amount in 2008. On a more strategic level, recently a wave of cyber attacks against NATO member Estonia in 2007, and then Georgia in 2008 have highlighted the crippling impact cyber warfare can have against a nation's critical national infrastructure.

We have experienced this threat close to home within the JSF Program, in which Turkey is one of the 9 partner nations. JSF is an industrial collaboration program, where the aerospace industries of 9 nations take part in the development and production of the aircraft. Given today's technologies, most of the communication and handling of aircraft data is conducted through online means. In April 2009, the Wall Street Journal reported that computer spies had penetrated the aircraft database and acquired terabytes of secret information about the fighter. Prime Contractor in the program, Lockheed Martin, later announced that while it faces continual cyber attacks, it has measures in place to deal with them and no classified information has been stolen. This incidence demonstrated the proximity of the threat.

Network Enabled Capability (NEC) came to be the basic concept in modernization of today's armed forces as a consequence of the information age. Turkish Armed Forces' military solutions embrace Network Enabled Capability (NEC) as a fundamental objective. To meet the requirements of Turkish Armed Forces related with interoperability and NEC, SSM is executing important projects, such as RADAR Network, Air Defense Radio Network, Link 16 Interoperability, Link 16 Terminal Procurement, Tactical Data Link Operation Center projects.

The concept of NEC is being studied in Turkey across the breadth of professional activities, including academia, industry, government and defense research. SSM has sponsored the first NEC Feasibility Study Report, prepared by experts from STM (Defense Technologies & Engineering Co.), faculty members from METU (Middle East Technical University), Prof. Dr. Erol GELENBE from Imperial College, UK and with the contribution of the Turkish General Staff. NEC Feasibility Study Report includes:

- National NEC concept,
- Similar NEC feasibility studies, operational scenarios,

- Technical design principles for the national NEC, models for the national maturity level, the evaluation method of the compatibility,
- Turkish Armed Forces' existing NEC infrastructure,
- National industry capabilities and
- Recommendations for the strategic road map.

The study report has been shared with the Turkish Industry and Turkish Armed Forces. We assess that NEC Technical Feasibility Study will be an important reference for the national understanding and future strategy. The development process of NEC starts with preparation of the National Vision & Concept for NEC document. The second stage is the reorganization which is followed by the document of National Targets and Master Plan. The next phase includes the national NEC architecture.

In order to guide the respective studies, NEC Collective Initiative Group has been established in 2008 with the participation of Industry, Academic and Research Institutions and Government Agencies to provide collaboration and coordination between organizations, and to provide conceptual, technical support and strategic advice. This group will also develop common terminology for NEC and propose common, effective and productive solutions, research and development projects.

Finally, National NEC Workshop is organized in November 2009 to introduce NEC Technical Feasibility Study Report results and strategic roadmap to Industry & Turkish Armed Forces.

In the concept of the network enabled environment, the vision is to associate different applications developed for different platforms and purposes in a common infrastructure, to provide user friendly and standard interfaces, to supply better communication and collaboration facilities and to transform all work processes in a common infrastructure.

The civilian provision of this infrastructure is the World Wide Web. The virtual information media for the defense usage will enable the multi-information and service sharing. In the prediction for the long term, all the defense platforms and applications will be covered. For the military,

information technologies are considered critical to many other technologies that support military operations.

There are several difficulties and challenges regarding the high level of the information assurance within network enabled environment. The effects of the attacks are experienced in the whole network. The information assurance level is provided at the same level of the least protected system. Probable security violations in a node existed in the single network will also affect other systems and nodes. In order to provide high information assurance within the network enabled environment, security actions shall be taken into account within all systems with physical layer, communication layer, network layer and application layer from a layered architecture viewpoint.

The second issue is different networks with different security levels. These networks will be connected into each other and may belong to Military or Civilian authorities in the NEC concept. The single or the dual direction of information exchange between these networks will be a challenge. In order to provide information exchange between all systems within the network enabled environment, NEC security policies shall be established and technologies shall be developed.

Realizing the critical priority of the topic, we organized the “Cyber Warfare” conference last December in Ankara to discuss the threats we face in cyberspace. Main topics discussed during this conference were:

- Understanding the risks faced against develop our communication and information systems through attacks or illegal access,
- Developing responses to cyber attacks and gather intelligence to prevent such from happening in the future,
- Improving coordinated response in case of attack.

As a result of this conference, we can mention following strategies for information assurance:

- Develop information assurance policies
- Initiate Cyber Defense projects
- Develop secure Service Oriented Architecture (SOA) approach solutions
- Develop new generation crypto devices

- Develop object level security solutions

I am sure throughout today's conference we will have hear extensively from subject matter experts on all these areas. This is a great event that attracts the attention of decision makers and industry within NATO and allied nations to the rapidly changing security environment regarding the cyber space and the vulnerability in information security. In this interconnected and interdependent world, it is clear that security issues are global and that nobody can address them alone. We cannot afford to be ignorant of these vulnerabilities. We must do all we can to mitigate risks and prepare ourselves to face future challenges.

In closing, I would like to thank you for this opportunity to speak to you. I hope that this conference will serve to expand our knowledge base and improve professional contacts. I wish everybody a very pleasant stay in Turkey.