2.1 Zero-Casualty War

A highly dynamic and intelligent battlefield surveillance and command and control capability has been developed, supported by a wide variety of on-line sensors and analysis, processing, and communications resources. This capability allows rapid deployment of forces armed with real-time intelligence to incisively respond to battlefield conditions with a minimum of casualties.

2.1.1 Scenario Description

A massive conflict has broken out between two Asian countries. Chemical and biological agents may be used. In preparation for a United Nations response, the U.S. has deployed networks of sensors in and around the conflict region. They include chemical sensors (vehicle exhaust fumes, urine, chemical agents, etc.), broad-spectrum acoustic sensors, seismic sensors, video sensors, and imaging sensors. Some are mobile.

A forward operating base is established in a neighboring neutral country to perform tactical reconnaissance. Terrain, street, and building information are updated based on visual and acoustic information from Unmanned Aerial Vehicles (UAVs). Signals Intelligence data are gathered from the UAVs and relayed to the forward operating base for analysis and correlation. Sensors provide acoustic, seismic, and visual signatures of each of hundreds to thousands of motorized vehicles that are cataloged and characterized. Air defense artillery and surface-to-air missile sites are identified. Automated analysis of visual information provides data about approximate numbers and locations of dismounted troops, enemy command posts, and command vehicles. Visual, chemical, and acoustical indications of weapons fire are all enunciated within the forward operating base, and video of that region is either initiated or tagged. Forward operating base data are relayed to the continental U.S. (CONUS). CONUS or forward operating base personnel can initiate video streams and live sensor reports.

While en route aboard transport planes, Future Future Combat Systems (FFCS) and Air Cavalry units monitor vehicle tracking information and dismounted troop movements and develop their unit plans. Up-to-date terrain, street, building, and weather information is loaded into FFCS and Air Cavalry onboard databases via satellite from CONUS and the forward operating base.

The mission succeeds with minimal casualties as a result of:

- Fusion of data from large numbers of sensors
- Large-scale target identification and tracking
- Large-scale video acquisition, transmission, analysis, and directing of this information to appropriate command and control entities
- Remote command and control of robotic surface and UAV resources
- Rapid insertion of overwhelming force

A key component of the mission is the transmission of critical, sensitive information over reliable, secure networks. The networks need to be rapidly deployable and configurable to support command and control as well as tactical operations.

2.1.2 Zero-Casualty War Networking Research Needs

The discussion of this scenario identified the need for research in:

Scalable networking for large numbers of low-data-rate nodes

Future combat systems will have thousands to millions of nodes with very low throughput, high delays, and high redundancy. Networking needs to support scalability to large numbers of nodes with very low data rates by allowing redundant nodes, highly sub-optimal routes, high tolerance to losses and errors, and adaptation to changes. Research is needed on programming techniques for large-scale redundancy-based computing paradigms.

Network self-organization, automated configuration, reconfiguration, and management

Dynamic configuration and reconfiguration of networks are needed to support rapid initial deployment of sensors and their networks, changing conditions and locations, and mobile elements with asset tracking and handoffs. To support these capabilities a wide range of information is needed such as topography, sensor location, and user requirements. It also requires network capabilities such as:

- Tool sets for network design and deployment
- Performance measurement throughout the network
- Network discovery of applications and their requirements
- Self-diagnosing, self-healing capacity

Research is needed to automatically generate, propagate, and maintain the optimal communications, network, and application configurations required to rapidly establish and maintain mobile ad hoc tactical networks. To support crisis or conflict situations, network resources should be deployable and configurable in an operational state in the time required to physically transport those resources to their destination. These situations also would benefit from an ability to establish *virtual* configurations of networking assets that may include mobile field nodes and fixed end user sites. This capability must support decisions about frequency assignment (optimizing spatial reuse), application location, and network addressing.

Self-organizing networks have the potential to reduce the large manpower requirements to set up and configure networks. Research is needed to reduce the number of networking infrastructure personnel required to establish, operate, and maintain networks from 20 percent of a rapid insertion force to no more than 1 percent of the force. This will require networking capabilities such as:

- Automated diagnosis and fault isolation of mobile ad hoc networks
- Non-destructive automated network reconfiguration mechanisms to maintain system integrity and performance
- Mechanisms for network evolution, including interface definition and standardization
- Automated mechanisms for the diagnosis and correction of problems in mobile ad hoc networks

Hierarchical networking

CONUS, forward operating bases, Task Force commanders, and FFCS cell team leaders have access to common views of the tactical situation, but typically need different networking and aggregation to operate at different levels of the hierarchy.

Seamless, transparent service across heterogeneous elements

In a dynamic ad-hoc environment, networking will rely on heterogeneous technologies (wireless, satellite, land line) that must seamlessly and transparently work together to support the end users. Network-to-network interfaces must be interoperable. Standards are needed to support seamless and transparent service.

End-to-end performance

Applications, networking, and services must cooperate to satisfy the end-to-end needs of the user in a seamless, transparent, cost-effective, trustworthy, and timely manner. The network must be able to adapt to mobile and ad-hoc sensors and nodes, accommodate in-situ sensors and nodes, and provide access to widely distributed computational resources (for example processing, modeling, and data resources). A knowledge-based, rule-driven tool is needed to tailor sensor performance to specific mission requirements and to tune the sensor array for deployment patterns, transmission frequencies, and power levels.

The networks need to support fusion of sensor data and to provide information tailored to end users requiring information at different levels of granularity – e.g., data covering a corps level or a battalion level. Sensor data may be aggregated in the field to minimize data transmission if the results will still meet end user requirements.

End-to-end performance measurement is critical to tuning end-to-end performance and trust.

Power management

Mobile networks will rely on finite power sources, usually batteries. It is critical that mobile network elements accurately measure and effectively use the power needed for sensing, processing, transmitting, and receiving information.

Trust: security, assurance, and reliability

Functions such as telemedicine, weapon's fire control, voice, and image transfers require high levels of end user trust. This trust will depend on end-to-end system reliability, security, responsiveness, and predictable performance. System responsiveness relies on channel access methods and end-to-end route generation. Predictable performance will require system and network redundancy and fault tolerance. Information must meet user and application requirements for trust by providing throughput, timeliness, fidelity, assurance, reliability, latency, location (e.g., for weapon's fire control), error, and other factors. QoS may address some of these factors.

Security must be provided throughout the system since each sensor and network node is subject to compromise. Differing levels of end user trust may accrue to different network paths, data aggregation from different sensors, cross-correlation of sensor data, and other system characteristics. Research is needed on decreasing information uncertainty through configuration and management of sensor and networking resources.

End user trust is dependent on establishing a common operational view and QoS. To achieve this, research is needed on:

- Techniques for capturing minimum mission requirements
- Adaptive middleware to map application-level requirements into network-level QoS mechanisms
- Network-level mechanisms (QoS and techniques) for resolving conflicting needs

Multimedia

Multimedia technologies will accommodate voice, data, video, and still images.

Revisiting networking fundamentals

Future systems will have to seamlessly integrate components with a dynamic range many orders of magnitude larger than today's networks (with speeds commonly ranging from hundreds of gigabits per second to a few kilobits per second) in a changing environment. Research is needed to revisit the network protocol stack to determine what types of control information are needed at each layer (including the application layer) to allow the other layers to effectively adapt to rapidly changing network conditions. Intermediate steps in this research include identifying characteristics of the potential links, interfaces, and component networks, and developing a control plane application/platform interface.