ASSURED NETWORKING IN NETWORK CENTRIC OPERATIONS

Anup Ghosh

Imagine an enemy in control of the chips that help fly our aircraft, drive our tanks and steer our missiles to their targets.

Imagine an enemy that can bring the mighty U.S. military machine to a grinding halt without ever deploying a soldier or firing a shot.

Imagine an enemy with the ability to turn the military's greatest advantage into our Achilles heel.

That enemy is not imaginary.

The vulnerability is real.

The computers and networks that form the cornerstone of future network centric warfare could become our greatest battlefield liability.

Our armed services can - and will - control the information space on future battlefields, providing our warfighters with a critical advantage over the enemy.

But make no mistake: We face a crucial crossroads in network centric warfare.

We can either continue incrementally improving our defenses against lowest common denominator threats.

Or we can change the game by fundamentally redefining how we do computing and networking.

If our ambition is truly to provide secure network centric warfare capabilities for our soldiers, then the choice is clear.

Today, I'd like to discuss some of the challenges we'll confront in protecting the military networks that make that information dominance possible - the vital information links between our solders, their commanders and the weapons and systems they deploy to win our wars.

I'll outline our vision of assured networking - the technology we'll need to transform computing vulnerabilities into secure information assets for our soldiers.

I'm aiming to enlist your support - to engage your knowledge and inspire your creativity - as we enter the transformative world of network centric warfare.

DARPA is certainly no stranger to the world of assured networking - in many ways, we invented the concept.

The first firewall was created by DARPA nearly 10 years ago.

Fifteen years ago, we responded to the first large scale worm - the Morris Internet worm - with the first Computer Emergency Response Team.

Today, many major IT companies in the United States could sport a "DARPA Inside" label - with many products based on DARPA-developed technology.

More importantly, the military is buying and deploying "DARPA Inside" network security products by the thousands.

Protecting information has always been vital to our military, but today the stakes are higher than ever before.

We have entered an era where attacks on information far transcend the cracking of codes for eavesdropping or the "hacking" of computer hosts to joyride through defense networks.

In tomorrow's battles, compromised digital assets could prevent U.S. forces from accomplishing their mission - literally, disarm our soldiers and prevent them from prosecuting the enemy.

Worse, a skillful enemy could turn our own weapons against us.

At DARPA, our job is to not only limit the vulnerability posed by information systems, but to transform today's liabilities into tomorrow's battlefield assets.

To achieve this goal, we are attacking the challenge from two angles: First, by building systems that inherently resist attack.

And, second - in the absence of perfection - building vigilance and intelligence into the network itself, so that networks can self-sense and self-heal to defeat attacks in real time.

I believe we can exploit Moore's Law of transistor densities and Metcalfe's Law of networking to create a secure computing fabric and an intelligent network infrastructure for the U.S. military.
To fully transform battlefield computing from a liability to an asset, we must start by building Trustworthy Foundations

Moore's Law gives us new chips with transistor density doubling every 18 to 24 months.
Up until now, the growth in transistor densities has been used almost exclusively to increase computing performance - whether through faster CPUs or more on-chip memory.
But what if we changed courses? What if we used the exponential growth in silicon real estate to redefine computer architectures ... to instill inherent security features within the core computing components?

Competing with Moore's Law is the trend that software becomes increasingly complex with time.
Yet the defect density of software remains fairly constant.
So as software grows more complex, we can expect bugs to increase in both number and complexity - a reality that makes applications harder to debug.
This results in a couple of "known knowns": We know that the software that runs our network centric warfare applications in the future will be buggy.
We know that buggy software enables both system failures and attacks.
And, therefore, we know that we must tackle the challenge of designing computing systems that provide a secure foundation to compensate for otherwise buggy applications.

In many ways, the architecture of today's computing systems resembles a house of cards.
One card is removed and the whole house falls in on itself: One component or application is compromised and the entire network fails.
We must begin designing systems with secure foundations, so that failure cannot cascade through a system and crash an entire military network.
Secure foundations can provide inherent robustness, allowing us to contain damage to small compartments, which can be either restored or compensated by other components.

To start moving in this direction, we need both the theory and the tools that allow us to build systems that are secure by construction - the same way geometry proofs are correct by construction.
Right now, we lack a provable theory that says: If I build a system from two or more trustworthy components, then the composition of them is trustworthy as well.

We also need to ask hard questions about the basic computing architecture we've been using for the past 30 years.

Is it time to scrap the Von Neuman architecture and develop novel architectures that are inherently secure?

Should we exploit the exponential growth in transistor density to enforce security constraints in hardware, rather than simply using them to grind out faster and faster computing cycles?

Can we build computer architectures that allow us to separate data from control? In the early days of telephony, the original "hackers" used those infamous Captain Crunch whistles to make free phone calls by emitting the right tones over voice lines.
The telcos got smart and separated control from data by creating a signaling network - a lesson we need to implement.

There are other promising technologies we can exploit in our quest for trustworthy foundations - but they require us to abandon traditional thinking.

Imagine a scenario where every task ran on its own machine.
If that task were compromised or simply crashed, we could design our systems to protect other tasks on other machines from the same fate.
But this "solution" would waste enormous computing resources on a machine that modern-day operating system kernels allow us to multi-task on a single CPU.
Instead, we need to design architectures and Operating System kernels that provide hardware-enforced protection of computing processes - so that the failure of one does not compromise others.

Obviously, building trustworthy systems requires the development of disruptive technologies - radical innovations that transcend traditional approaches.
But the fate of disruptive technologies in the market is highly uncertain - a few succeed, many fail.
So we need to figure out what determines the fate of disruptive technologies in the commercial marketplace - what factors lead to commercial success and what circumstances lead to oblivion.
And we need to create economic and marketplace incentives to foster the disruptive security technologies we need - incentives such as establishing APIs and open standards, promoting industry consortia, ensuring a critical mass of both consumers and manufacturers, and developing meaningful certification and accreditation standards.

Rapid advances in technology - such as the coming revolution in programmable logic devices and customized devices, and our increasing ability to dynamically reconfigure devices "on the fly" - allow garage enthusiasts to compete with the largest industrial firms in developing sophisticated, innovative architectures and devices.
Our challenge is to tap into this confluence of technology and talent to prototype and validate novel architectures for secure computing, quickly and efficiently.

Let me shift gears for a moment and discuss the second prong of our strategy for protecting military networks: creating vigilant autonomic networks.

While we need trustworthy foundations for computing, we also need our networks to be vigilant and autonomic in the face of attacks.
The threats we face today render human-in-the-loop response untenable.
Worm-based threats can saturate enterprise and battlefield networks in the blink of an eye.
While worms pose serious threats to the Internet, the consequences for code-driven threats like worms for military networks are significantly higher than lost revenue.

Military networks have special challenges that stretch the limits of our current thinking.
Battlefield networks are mobile and ad hoc, not static.
The topologies they operate on are dynamic, not stable.
Group membership changes frequently, along with the terrain, affecting both physical and logical network boundaries.
In the tactical battlefield environment, failure and the unexpected ARE the norms.

At DARPA, we have a destination in mind -military networks that have the vigilance to sense when they are under attack, and the wherewithal to recover and reconfigure around failed and compromised components.
In other words, we need to design the network to be its own autonomic immune system.

That means building intelligent networks that are self-organizing, self-sensing and self-healing -- networks that assemble just-in-time, all the time ... that sense and repulse attacks ... that repair and reconfigure themselves reflexively ... and that can accomplish this mission without an American soldier ever having to intervene to administer their systems.

Let me put an even finer point on it.

With traditional networks, failures occur, users notice, and then an IT tech is sent in to repair the problem.

Users only learn of an attack after a failure has occurred.

And the repair requires human intervention that usually takes hours or days.

That won't work on a battlefield where the potential consequences of down time are several orders of magnitude more catastrophic than missing a few emails or losing Internet access.

Today's military requires the network, not the user, to sense the attack.

That means routers and switches must recognize and respond to denial of service attacks ...the network must sense malicious code, network worms, and malicious insiders ...clusters of nodes must have the ability to autonomically reconfigure themselves on the fly and dynamically provision services as needed to compensate for failed nodes in order to accomplish the mission.

We've made great progress creating mobile networks that are able to self-form and re-organize as needed when comm links fail.

We need to extend these concepts to dynamic reconfiguration of the network in the event of attacks and failures against hosts.

For example, if a computer worm were unleashed on a mobile-network system, we would need the network to sense, quarantine and reconfigure the network to contain the worm spread, while still providing the mission-essential functionality.

Obviously, we're searching for solutions that leap frog traditional firewalls, crypto and anti-virus technologies.

There is no reason to believe that a linear evolution of today's thinking will lead us to the technology we need.

Instead, DARPA needs new methods to address new challenges.

As we move to the peer-to-peer vision of networks that vision will require a new paradigm for sensing and repelling attacks based on technologies only dimly conceived today.

Network Centric Warfare and Network Centric Operations have been billed as "the cornerstone" of the Defense Department's strategic plan to transform our armed forces.

The Pentagon believes that, in future conflicts, the network will be "the single most important contributor to combat power."

Think about that: "the single most important contributor to combat power."

Our ability to link our armed forces and systems together in a seamless and protected communications chain will contribute more to America's warfighting capabilities than any weapons systems or piece of military hardware.

In other words, in this day and age, the network is the weapon.

Our goal today is to inspire you with a vision to shape the future of information technology to enable network centric warfare and to challenge you to generate the ideas and systems that will realize this vision.

We are asking you to re-think the way we currently do computing and networking, to re-invent the future in a way that only DARPA would dare pursue.