

J.B. “Gib” Godwin Addresses the 2010 Spring East Coast conference on Cyber Security



J.B. “Gib” Godwin
Vice President, Cybersecurity and Systems Integration
Northrop Grumman Information Systems
Defense Systems Division

On Tuesday, March 23, 2010, J.B. “Gib” Godwin, vice president, Cybersecurity and Systems Integration, Northrop Grumman Information Systems addressed the 2010 Spring East Coast conference on Cybersecurity in Washington, D.C. Below are his prepared remarks:

On behalf of Northrop Grumman, I want to thank you for inviting me to address a major threat facing every aspect of our economy and our national security apparatus today.

Today, I’ll be talking about the nature of the threat ... and our vulnerability.

I’ll propose a new paradigm for responding to this threat.

And I’ll talk about how Northrop Grumman is already implementing this new paradigm.

But before I get started, I want to offer a little history lesson.

So you all remember the Lone Ranger. WHAT? You don’t. I guess I’m showing my age here. Well, those of us of a certain age can never forget the excitement:

The William Tell Overture plays, and then comes the announcer: “A fiery horse with the speed of light, a cloud of dust and a hearty ‘Hi Yo Silver!’ The Lone Ranger. ‘Hi Yo Silver, away!’ With his faithful (Indian) companion Tonto, the daring and resourceful masked rider of the plains led the fight for law and order in the early west. Return with us now to those thrilling days of yesteryear. The Lone Ranger rides again!”

Not only did we know the Lone Ranger, we knew all of what we would today call the “brand attributes.”

The palomino horse, Silver, of course.

The white hat.

And perhaps most important, the silver bullet, reflecting the character of the show’s hero. The preciousness of the resource used represented the preciousness of human life. Because a silver bullet meant one shot, rarely used, the term “silver bullet” came to signify one-shot solutions to a difficult problem.

War-fighting used to be like the Lone Ranger. On TV, you always knew the bad guys by their black hats. In war, they were in the other uniform.

In both war and with the Lone Ranger, strategy and surprise played a role – he was, indeed, “daring and resourceful” – but the battle was still fought out physically and superior force and will carried the day.

But we can’t simply return to those thrilling days of yesteryear. Because today we are facing a very different kind of threat – and a different kind of fight.

In this fight, there are “no silver bullets” – no single, one-shot solutions. Because this threat is so big and fast-moving, so diverse and sophisticated, that it’s impossible even to refer to a “solution.” It’s more about “responses.”

There are no silver bullets with the cyberthreat because there is no single source. It is indeed the wild west out there ... but the bad guys are not out in the open wearing black hats. The cyberthreat is a really a range of threats including everything from teenage hackers ... to superpowers ... and everything in between.

Consider some of the headlines that popped up in a very short period of time earlier this year:

- “Twitter Hack Part Of Broader Iranian Strategy”
- “China accused of cyber attack on Google”
- “\$26 Software Is Used to Breach Key Weapons in Iraq”
- “North Korean hackers may have stolen US war plans”

There are no silver bullets because there is no “sample” attack. This slide presents some of the key ways intruders are targeting systems today. The lower left represents the classic distributed denial of service attack.

These attacks are launched from networks of thousands of bots... computers that have been infiltrated and enslaved as platforms for remote cyberattacks. These bots are employed to overwhelm a server and slow or interrupt its performance.

By the way ... the going market price to acquire access to a such a bot? As low as 4 cents, according to Symantec.

The Facebook screen represents the increasing sophistication of another threat ... so-called “phishing,” or emails disguised as legitimate mail but carrying malicious code.

These emails are becoming so targeted and well-written that they are hard even for trained observers to identify, a phenomenon that is being called “spear-phishing.” The reason is that data on targets can be aggregated from so many public sources ... from social networks to directories to tracking behavior online, the equivalent of figuring out the launch of Desert Storm based on the number of Dominos Pizza deliveries to the Pentagon.

The word is that a Facebook password ... with all the valuable private, personal information it opens up ... can be had for around \$200.

The thumb-drive represents so-called “supply chain” attacks, where goods or equipment – perhaps a thumb drive innocently accepted at a trade show – contains malicious code. It’s why many defense installations and contractors had previously barred the use of memory sticks.

Finally, there's the website. Hackers are now embedding malicious codes in websites popular with specific groups – the State Department was infiltrated in exactly this way.

There are no silver bullets because there is no simple vulnerability. I'm going to show my age again by quoting an old cartoon character, Pogo: "we have met the enemy, and he is us."

I'm in the business of information systems for defense. But it's clear that those same sophisticated information systems that have given us an enormous advantage militarily have also opened up new avenues of attack, against both our defense and civilian infrastructures, and created a range of vulnerabilities.

We're victimized by **gaps and overlaps** in our systems ...Where our forces' systems are integrated, we see and defend against a problem once. Where they are not, we provide 1000s of targets for that same probe. Multiplicities of networks and software also mean multiplicities of vulnerabilities that can be attacked by malware.

We're hurt by **our open ranges**: the openness of our democratic culture also provides more freedom to roam around the Internet and enter into personal and business networks and systems.

Another vulnerability is the "**clueless and careless.**" Like a chain with the weakest link or an army with the slowest soldier, our security systems are only as strong as the most casual employee in our organizations when it comes to cyberdefense.

We're vulnerable because of the asymmetric nature of the threat ... attack is cheap, defense is dear.

But perhaps the biggest area of vulnerability, as I'll elaborate later, is policy. The kind of deterrence we know in conventional warfare presents a challenge: it's hard to deter an enemy you can't see.

And with economic loss or mere inconvenience frequently involved, as opposed to physical harm, the question of **how, where, when, if to** respond – or even attack – is a highly sensitive issue.

There are no silver bullets because there is no "superior force." We can't hope to stop everything because the threat is continually bigger ... faster ... and smarter.

The attacks are bigger – It wouldn't be an exaggeration to submit that if this is war ... and it is ... we are up against the largest standing army in history. The president of our Information Systems sector has pointed out that the massive scale of today's cyber attacks place them on the level of warfare.

In fact, we experienced a 152 percent increase in the number of cyber attacks on the US government in 2007 alone ... and a 55% rise in intrusions on military networks.

As a result, each and every day there are an estimated 360 million probes directed at Pentagon computers, looking for vulnerabilities. That comes out to more than 4000 every single second. I talked about botnets – well, Symantec tells us that there are now more than 9.4 million distinct bot-infected computers ... and that more than 75,000 of them are active on an average day.

And a further measure of the magnitude of the threat is seen in a coordinated attack on government networks last year. It involved nearly 170,000 zombie computers in 74 countries ... consuming between 20 to 40 gigabytes of bandwidth per second. It managed to hit virtually every major Federal agency, including the White House. And that was considered a relatively MINOR attack.

One look at this chart will tell you what I mean when I say that the cyberthreat is moving faster. In a single year, 2008, the number of malicious code threats extant grew 265 percent. More than 2800 new codes were produced every day last year.

Consider that it takes code writers months at a time to analyze these codes and produce and distribute patches for them. So you can see how the threat is evolving more quickly than the response ... we won't recognize the world we're in five years from now.

And the attacks and the attackers are smarter. Consider the botnets I've discussed. Increasingly, even as we identify and interrupt them, they have the ability to go underground and reconstitute themselves using other computers. They will attack and probe systems using adaptive tools which are increasingly automated and become smarter as they are defended against.

How smart are these probes? A Northrop Grumman team conducted an experiment in which they simply took a computer with the most robust commercial security software available, connected it to the Internet and did nothing.

It took just four hours for probes to begin, and within two weeks the computer was taken over by a server in Canada, which was in turn run by another server in Singapore, which was in turn controlled by another server that could not be traced. The computer was used by parties unknown to attack another computer in Poland.

So there are no "silver bullets" because there is no single source, no sample attack, no single vulnerability, and no superior force. And there can be no "Lone Rangers" either ...we're all in this together.

Everyone's interconnected ... one sector's, Department's, service's or ally's vulnerability is everyone's vulnerability.

Multiple lines of attack must mean multiple lines of DYNAMIC defense. And the asymmetric nature of the threat – the ability to mount crippling assaults for pennies – means we must pool resources to divide and conquer.

So if there are no silver bullets ... and no Lone Rangers ... what is the proper response to this ever bigger, faster, smarter and more diverse cyberthreat?

I want to suggest today that we need to respond by moving to an altogether new paradigm of cyber assurance: a holistic approach to electro-magnetic spectrum dominance. And perhaps the best way to understand this new paradigm is to line its characteristics up against those of the old paradigm.

The old paradigm is to defend: our enemies and others disrupt the spectrum and use it against us. Meanwhile, we huddle behind a "Maginot line" and try to stop them.

The new paradigm is to dominate. We control the spectrum and use it to advance the mission.

The old paradigm is reactive. We're on the receiving end of attacks and respond to them. But even then, we're not sure what has hit us and from where. We lack the ability to understand and evaluate the threats we're facing.

The new paradigm is predictive. The real opportunity is not simply sitting back, waiting for attacks, responding to and defending against them, as vital as that capability is and will remain. It's in identifying and understanding the enemy ... and anticipating, preparing for, precluding, and even, in the appropriate circumstances, pre-empting attacks.

Cyber assurance in the old paradigm is fragmented. Cyber assurance has for too long lived in stovepipe communities. We create increasingly artificial distinctions among cyber, electronic warfare and kinetic forces. Which ultimately puts the enemy in a position to divide and conquer, to take advantage of those gaps and seams and find our weaknesses and vulnerabilities. This fragmentation also means that attacks faced by various, fragmented stovepipe communities are threats of first impression, even if they are known to other communities.

The new paradigm is holistic. It's about cooperating, collaborating and coordinating across the electro-magnetic spectrum: From air to land to sea to cyberspace.

Because we recognize that it's not just computer networks we're defending: it's sensitive weapons systems, vital communications and critical intelligence capabilities that guide our forces. And in fact, our success in dominating the electro-magnetic spectrum can have impact beyond the defense sphere.

That's why if it's a tron, we need to be able to manage and use it ... offensively, defensively, exploitatively, and as I have just said, predictively.

This holistic approach ends our counterproductive and even dangerous line-drawing and brings together cyber with EW as well as non-electronic sources of information ranging from FME, MINT, OSINT, MASINT, HUMINT and political and economic analysis. And it combines exploitation and exfiltrate information with the detection and defense of intrusion ... and stop attack with offensive capabilities.

More specifically, the old paradigm of cyber assurance is **network-focused**. It's about protecting the computer network at any cost. The new paradigm is **mission-focused**. It's not just concerned with what's happening to the network, but also to the war-fighters and systems that are depending on that network in the field.

Because it is so focused on the network, cyber assurance in the old paradigm often **compromises the mission**. To seal off and stop an attack, we shut down the firewall, repair the damage and eventually reopen it ... leaving our war-fighters flying, sailing, and rolling blind during shutdown.

The new cyberassurance paradigm "**prioritizes the mission.**" We're building the ability to operate under attack through the concept of "dynamic defense." We need to assure that command/control/ communications functions are secured 24/7. Dynamic defense capability involves redundant systems, re-provisioning to keep fighting ... or operating ... through a threat, and the ability to migrate C3 functions to different pathways.

In the old paradigm, cyber assurance is an **add-on**. It's an afterthought, bolted onto legacy systems, which are too costly to throw out.

In the new paradigm, cybersecurity is **integrated**. The bottom line, once again: to get the right response against a bigger, faster, smarter threat, you need to ask for capabilities that are up with and up to the challenge, while building in the requisite flexibility as well. All future acquisitions must integrate Cybersecurity. There must be a cybersecurity information assurance element to all future platforms and weapons systems and communications platforms, in the air, on land and on sea. Cybersecurity must be part of the thinking, part of the planning, part of the requesting and ultimately, a central part of the capability from word one.

In the old paradigm, cybersecurity is **improvised**. Not only are we outgunned and outmanned by the world's largest standing army, we're out-prepared. We lack the trained personnel to own the spectrum, which leaves inexperienced and unprepared teams making it up as we go along.

In the new paradigm, our teams are **trained**. We need to develop the ability to train a large force in a cost-effective way ... and the best way is to do training on-location in small sessions.

The old paradigm, to coin a phrase, is about **the geek squad**. Cyberwar is too important ... and too sensitive ... to be left to the technologists. But the truth is that technologists are leading the response with policymakers often in the dark. The lack of policy input ties our hands in developing strategy and solutions – because we don't know what ultimately will fly and won't.

The new paradigm, therefore, is **policy-driven**. We need to have informed policymakers setting the parameters, allowing us to develop the technologies to carry out policies and strategies, instead of the other way around.

In the old paradigm, Cyber assurance is **isolated**. It's too frequently confined to the point of attack, duplicative and expensive, with no knowledge or benefit of understanding the attacks with which others have dealt.

The new paradigm is coordinated – it's about **“faithful companions.”** We need to work with our kimosabes – our allies – and sometimes even the guys in the black hats. We need to work with partners in academia and across the private sector, to pool our resources and share information to counter low-cost attacks and advance learning and understanding. And we need to work with these partners to divide up our responsibilities and counter multiple lines of attack.

Which brings me to the final focus of my comments today ... some of the initiatives Northrop Grumman is pursuing to advance this new paradigm of dominating the electro-magnetic spectrum.

To begin with, we're making extensive investments in a best-in-class, emulated closed-range system to identify and design approaches that allow us to get out in front of the threat, maintain the mission and dominate the spectrum. In state-of-the-art laboratories, we're creating scenarios that define our vulnerabilities, emulate enemy attacks and develop responses ... or maybe I should say “pre-sponses.”

We refer to emulation because these capabilities go beyond simulation. We're recreating the real-world environment to the highest degree practicable in closed system, driving to total failure

to ensure we have a complete grasp on the impact attacks will create on systems and how to keep operating through them.

These emulated ranges provide another extraordinary advantage – they allow us not only to develop pre-sponses but to put together training sessions that truly prepare our teams for the most cutting-edge threats. And since these ranges involve a distributed system, we can do and are doing that training as I suggested earlier – on site, with small groups of cyber warriors across DOD, the government and industry.

I might add that Northrop Grumman offers a complete range of Cyber Warrior courses ... where we train and qualify team members at various levels to be experts and leaders.

These eight courses – ranging from overview courses for non-technical officers and staff to in-depth, comprehensive courses for specialists – cover the latest computer network threats, tactics, defensive measures, and certification and accreditation processes.

And of course, we've pursued and are sharing with clients aggressive programs to provide training and heighten awareness of, and sensitivity to, cybersecurity in the general employee population. Even at Northrop Grumman, leaders in dealing with cyberthreats,, we continually need to train employees to be savvy to the simple email and other intrusions that can take down a system.

We're Integrating Cyberassurance into the acquisition process. Our emulated ranges allow us to do smarter acquisition because we have defined our vulnerabilities and possible responses to the ultimate. And to address the down-and-dirty, nitty-gritty practicalities of this element of the new paradigm, two of my colleagues, Dennis McCallam and Ken Brancik, have put together a white paper. The paper focuses on critical criteria for cybersecurity and how they can be written into Section L and M of the Instructions for Proposal Preparation.

Looking forward, we're undertaking tests of a process to meet fire – an asymmetric threat – with fire: the Asymmetric All sources Analysis Against Persistent Threat or A4PT. A4PT is the new paradigm in action. It is completely conceived around the need to take a broad range of intelligence and other information and develop knowledge of the sources of attack ... not only now but in the future ... and not only in the context of protecting the network, but more important, in the context of assuring the mission.

It combines and deploys data from all sources, including not only the terabytes of data coming at networks, but also ... as I suggested earlier ... FME, MINT, OSINT, MASINT, SIGINT, HUMINT, and political and economic analysis. Then it takes this data and subjects it to complex event processing, systems that have been used in the financial world to provide real time analysis and response in trading situations . The CEP system sorts– as our farm-sorters symbolize here – the important from the unimportant and analyzes the results in the context of the entire vault of information.

We're expecting to have more specifics from these A4PT tests to talk about in the near future. But the objective is clear: to deliver reliable information and responses – developed in anticipation of a specific scenario – not only to cyberwarriors but also to our war-fighters on land, in the air and at sea. Such a proactive, holistic approach removes the air, igniter and fuel for the fire for the cyber attacker ... and allows us to get ahead of the enemy, not just react.

Meanwhile, to tear down those stovepipes – we’re engaged in a broad range of information-sharing and public-private partnership activities with various kimosabes: cutting-edge academic centers, providers of commercial security products, industry partners and foreign governments.

For example:

- Our Cyber Integration Center is working with other industry partners to conduct cyber war games for the Air Force
- Our Chief Technology Officer, Dr. Bob Brammer, has created a Cybersecurity Research Consortium with leading academic centers including MIT, Carnegie Mellon and Purdue
- But because kids are already so clued in these days, we’re starting even earlier than that. Our CyberPatriot program is a relationship among Air Force and industry partners to go into high schools to conduct cyber-war games.
- We’re involved in numerous partnerships with small, cutting-edge companies.
- One key partnership – our TRIAD Network – is at the core of our InfoShield product, which is where we combine our internal and external expertise and incorporate it into a holistic Information Security Program for our clients. TRIAD – which stands for Transformational Research, Integration and Demonstration – is a state-of-the-art network of 47 Laboratories in 20 locations nationwide. TRIAD enables our customers to investigate the latest technologies, test new products and innovative ideas, and validate solutions.
- And to further reach across stovepipes, along with several of our defense contracting competitors, we also participate with DOD and the defense ministries of the Netherlands and the UK in the Transglobal Secure Collaboration Program. TSCP focuses on a common framework for sharing of sensitive information in international defense and aerospace programs.

Most important, we’re involving ourselves in initiatives to get policymakers at all levels out in front of the process in cybersecurity ... so that technology is following strategy. One example is our cooperation with the George Washington University Homeland Security Policy Institute. HSPI is focusing on bringing together leaders from the administration, the legislative branch, as well as international policymakers, and advocating the development and articulation of a clear cyber doctrine. One of our Corporate executives serves as a senior fellow at the Institute.

So to summarize:

1. The Cyberthreat is too big, diverse and fast-moving for silver bullets or Lone Rangers. We’re facing the largest standing army in history, one that is using its size, the incredible reach and low cost of its technology, and our own openness and vulnerability to probe, divide and conquer us.
2. To counter this threat, we must move to a new paradigm: a holistic approach to electromagnetic spectrum dominance that is pro-active, predictive, prepared, coordinated, integrated, mission-focused and policy-driven.
3. Northrop Grumman is investing in predictive, knowledge-based responses, emulated, closed-ranged systems, training and far-reaching partnerships to position America to achieve mission assurance and spectrum dominance.

And most important, we want to work with everyone in this room to take command of this threat ... to get America, its war-fighters and our people off the defensive and back in control of our cyber-destiny. Because there are no Lone Rangers and no silver bullets, I look forward to talking to many of you during this conference and sharing knowledge, ideas and responses.