Mr. James Gosler
Fellow, Sandia National Laboratories

Cyber Threats – The Digital Dimension

Note: Below are informal notes taken by a JHU/APL staff member at the Seminar.

Mr. Gosler noted in his introduction that his remarks would be only his own and did not necessarily reflect the opinions of any official organization. He also stated that his talk had grown out of a study of defensive challenges to a specific government entity. The study showed that the organization had no real threat-based investment strategy. Without such a strategy much of its huge offensive budget could be wasted since no one knew how a sophisticated adversary would play the game.

This briefing is on how sophisticated adversaries could operate to cause both disruption and integrity issues

- Briefing also could be given at a much higher level of detail but would require higher classification
- Longer versions (up to 7 hours) used similar viewgraphs but with more detailed assertions
- Classified details can put meat on the bones of the assertions made here
- If this topic is of interest, arrangements could be made for more in-depth briefings to individual organizations at other classification levels
- Briefing provides a way of thinking about cyber and related threats using info you already know

Two books by Jennifer E. Sims and Burton Gerber provide excellent background at the unclassified level

- Transforming U.S. Intelligence (2005)
- Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence (2009)

Principle Assertion: Against a sophisticated (average) adversary, the current state-of-art in Information Assurance is significantly out matched

- Rest of talk will show how important this is
- Can be somewhat counterintuitive at times
- Even an adversary with only average capabilities could have great advantages in these areas
- Gap between defense and offense is large and growing – was biggest threat before the financial crisis
- Others have believed in the same assertion
  o ADM Bill Studeman (Former DDCI & Director of NSA / Member, WMD Commission
  o Don’t need to be a rocket scientist to understand the problem
- Obvious that principle adversaries understand US vulnerabilities related to our need to have software work exactly as designed
- General Cartwright at STRATCOM has noted the problem
- Absurd to keep building critical systems as if they were not subject to attack
  o These systems will be operating in threat-rich environments

Can use analogy from ship-building

- We don’t build warships to go as fast as possible or to carry as many guns as possible
- Must take other things into account to keep a balance such as habitability vs. weapons numbers
- Trades of one capability versus another always need to be made
- Some potential problems of ships are avoided by a built-in redundancy of systems
- Other vulnerabilities are handled by extensive and continual training of the crew in damage control
- Bottomline: Need to do something similar with trade-offs when designing critical electronic systems
  o In ship design these trade-offs are handled at the platform level
In systems design critical equipment relies on off-the-shelf parts/sub-systems to mitigate problems with development speed and costs without concern for possible adversaries’ actions.

Adversarial Innovation is another area that is largely neglected.

- Can be done simply by looking at a problem a different way than what was used to design the system.
- Depends on the type of person involved: Twisted / Twistable / Hopeless.
  - At CIA there were many people with history/international relations background
    - Looked at things differently than those in Gosler’s Navy/Sandia experience
  - Must have a mix of people to process all of the information we are now faced with
    - Some would stay at the gate in the picture all day – play by the rules
    - Some would not hesitate to go around the gate
  - Must work out what percentages of each kind of people needed to handle complex info processing.

Another complication is that the offensive side always gets to choose when / where / how to attack.

- If they invest enough in target analysis, they will identify the easiest targets.
- Will use a cost/risk calculation to find which options give them minimal cost/risk.
  - Somewhat dated now, written by a Soviet spy who is now an American citizen.
  - Describes the creative teams who understood those 3 types of people.
  - Soviets compromised the systems of one country for years without the target knowing it.
    - US did not know it until spies told them.

In 1984 Ken Thompson (Bell Labs) wrote *Reflections of Trusting Trust*.

- Basic assertion: You can’t trust code that you did not totally create yourself.
  - No amount of source-level verification can protect you from untrusted code.
- In 2005 Gosler went a step further in *Transforming Intelligence: The Digital Dimension* with the basic assertion: “You may not even be able to trust code that you totally created yourself!”
  - Software code is now so complex that you might not be able to believe that all you wrote was right.
  - Software designers might trust their code but would could not fully verify the equipment it ran on:
    - Micro-electronics can be compromised, too.
    - Also could not fully trust the connections between software and hardware.
- Complexity keeps increasing beyond any way to fully check software/hardware/etc.
Mr. Gosler noted that he had a hard time keeping the right side of the viewgraph current because of the rapidity of improvements today

- Moving from discrete electronic devices to micro-electronic sub-systems for major equipment adds complications
- With micro-electronics you are less likely to be sure about all the sub-elements involved
- It used to be possible with software to go line by line to check that everything was correct
- With the type of testing that can be done today, testing the elements of the right side of the slide would not bring things up to the standards available from the systems listed on the left side
- A very good malicious code builder could do something that 4000 evaluators could not find
  - Having many evaluators may not be a sufficient strategy to provide forensic evidence, but it is necessary one

Who has access to the secrets can be just as important as evaluating the software/hardware

- Spies have done the most damage from their positions of trust
- Usually, we only find spies on tips to counterintelligence agencies about information in the wrong hands
  - Then they must determine who had access to the info
- If you give a scumbag a position of trust, no amount of evaluation would be enough
  - So must do a lot of vetting of people working in the system
- Need to put as much investment in technology to ensure that what it is doing is correct as what goes into the basic design

Domain of Vulnerability

- An adversary could steal intelligence by technical tricks such as from network buffer overflows
  - A great deal has been invested in making sure that this does not happen
  - Even Microsoft has been doing a lot, but not enough
  - Involves protecting with technological barriers such as firewalls, intrusion detection systems, etc.
- Sophisticated adversaries could use some very inexpensive ways to attack
  - They will always find some vulnerabilities
- During Soviet days, top-of-the-line IBM Selectric typewriters were modified before they reached the US Embassy in Moscow so they would transmit what was typed
  - Shows need to protect everything in the domain
  - Typewriters were modified while still in the supply chain
- Bottomline: There are lots of places to compromise equipment or software; hard to identify changes
Characteristics of a Sophisticated Offensive Organization

- More than just clever hackers who could cause some harm to the US (but not bring it down)
- Have global presence with wide options for acquiring resources
- Use good tradecraft – what spies do to make you not know that they are working against you
  - Spies usually get caught after they get lazy and don’t follow their own tradecraft rules
- Have networks of trusted partners at least for temporary missions
  - Partners may not like each other that much but both hate the US more
  - May also have some untrusted partners

Risk management is hard to do and getting harder in this field

- Adversaries have more and more access to the systems that we depend on
  - Much software / hardware now being designed and built overseas
- Brain trust issues: We’re getting dumber while they are getting smarter
  - Problem has been reported in a National Academy of Sciences study: Rising Above the Gathering Storm: Energizing and Employing America for a Brighter Economic Future
  - Study concluded because of so much foreign input in all critical systems, it would be impossible to do enough evaluation to overcome the problem
- Our dependence on these systems is growing – Why buy some item carefully built here for a $1,000 when an OTS version from elsewhere might cost less than a dollar
- Adversaries are often better at offensive efforts than we are in these fields
- US is losing its lead in many fields
  - Example: In an undergraduate math team competition only two US universities were in the top 40 competitors
- Adversaries are increasingly employing smarter, hungrier people who may want to cause the US grief

A notional way to look at adversary capabilities – rank levels of technical and operational competence

- Clever hackers would be given a score of 1
- Teams of criminals would be worthy of a score of 30
- Sophisticated, sponsored adversaries would reach a score of 1,000
  - They do not need to play at this level all the time to win
  - They will play just above where they think they need to be to win
  - Some may be somewhat risk tolerant and some may not care about the risks at all

Example: Project Gunman – Soviet modifications to IBM Selectric typewriters

- Best machines went to the most important people at the Embassy
- Everything typed was transmitted to nearby listening post
- Very subtle change would not have been noticed by an experienced repairman
- All done quickly during transit in the shipping channel

Situation is gloomy – need to stop the gap between offense and defense from expanding so must rethink ways

- If I make this investment, will I increase the probability of finding those hidden problems?
- If I am capable of finding a problem, will I be able to tell who has caused the problem?
- If I find the problem and identify the adversary, can I create consequences against that adversary?
  - Anything done to the adversary must be disproportionate to ensure it does not happen again
- If a piece of equipment was designed better, perhaps with redundancy, impact would be less to the US
  - Let adversaries know that if you mess with me, I will still have enough in reserve that it will not be worth your effort to try
  - Basic point to put across to the adversary: Don’t do it
- Bottomline: It would be better to use a more offensive strategy and it might not be worth investing in some defensive efforts

Changing the culture is the hardest part of trying to improve the situation

- Many senior people in government are usually in denial about the need for change
- Louis V. Gerstner in Who Says Elephants Can't Dance?: Leading a Great Enterprise through Dramatic Change:
“Successful institutions almost always develop strong cultures that reinforce those elements that make the institution great. They reflect the environment from which they emerged. When that environment shifts, it is very hard for the culture to change. In fact, it becomes an enormous impediment to the institution’s ability to adapt.”

- Now there are many senior people in government who understand the problem/willing to look for solutions
  - There had been over the last few years
  - Feared the critical mass needed to make changes would be lost in new administration
  - Appears that there are enough who understand and are willing to lead change

- First must recognize how quickly long-standing situations can change
  - Army-Navy football game program in 1941 stated the significance of the fact that “no battleship has yet been sunk by bombs” and was illustrated by a picture of the USS ARIZONA
  - One week later the ARIZONA was sunk

- Change can take place but it might need unusually large effort
  - LT Sims in the mid-19th Century US Navy had suggestions about how to significantly improve gunfire at sea based on Royal Navy improvements
  - No senior people would listen to him leaving him extremely frustrated
  - Took his concepts to President Lincoln directly, was finally heard and changes were eventually made
  - Bottomline: changing a well-established culture can be very difficult

Concluding Observations
- Could not provide justifications for the assertions made in this brief at this classification level
- It will not be easy to solve these problems
- Technology alone cannot handle the problems
- Political changes will need to be made
- National Defense Strategy is not sufficiently informed although it is much better than was a few years ago
- US cannot win using only C+ students
  - This is not the only problem affected by student achievement issues

“Most important” slide in the briefing:

- Speaker has been working on getting the two sides of the graphic to move toward each other
“Cyber” is not a good term since it is too limiting
If you have cyber tools you want to use them to target cyber activity
  • Reasonable to assume that you would use tech/cyber methods to handle these problems
  • But burglars / spies also are used against cyber targets so must defend against them, too
Must also have partners you trust and some you don’t trust in all circumstances
If you believe that you can defend cyber targets with only cyber and tech tools, you’ll lose
• Partners can be surprising – may not even know they are partners
• Adversaries can change the rules of the game
• Different groups play in different areas but may not work with those facing similar threats in other areas
  • Such situations develop seams that the adversary can exploit
  • Need an integrated team to work across all threat areas
• If you only throw small amounts of money at various methods of protection, you will only get incremental improvement

Conclusion:
What has been presented here is only an outline. You need to take what you know and what you need to learn and place all of that within this template.

QUESTION & ANSWER SESSION

There are only a handful of very sophisticated hackers and they could cause some problems
• See DNI Blair’s recent testimony on this
• Sophisticated adversaries can work at a much larger scale
• Hackers also cannot get us out of the problem
• Terrorists and non-state actors could cause us problems but not on the huge scale that sophisticated adversaries are capable of

There are some technical partial answers to the untrusted code problem
• Devices might be made overseas but would be programmed here in trusted circumstances
  • Doesn’t solve the problem but does help
• Also have the problem of denial of services because something is made not to work properly
  • It does not take much to make things not work
  • Our dependence on micro-electronic equipment is part of the problem

Information Assurance efforts can also be a response to the problem
• Red Team efforts are called inadequate in this brief so talked to some
• They wanted to be raised to the “50” vice “30” mark but marks are only indicators
  • The 1,000 level for a sophisticated adversary is really more like 10,000
• These are just notional efforts to scale a problem that is very large

Using the concept of “keep your friends close and you enemies closer” would be a good idea
• But it is hard to keep enemies close
• General concept is under some discussion at the moment
• Adversaries have the same problem
  • However, the impact on them is less if their defenses fail than if our offenses fail

Two different types of threatening objectives
1. Compromising confidentiality
2. Denial of services
What you do to protect against one problem can make matters worse for the other problem

Culture Change Problem
• The military is often tied to scenarios that they have built
• Gamers can’t let cyber issues take over and stop the scenario playing
• So think that there is need of a cyber Pearl Harbor before things are changed
  • It looks as though there should be enough evidence already out there, but there isn’t
• Some things are not being done that could be done because the cost or the pain are too great
• Must ask how much more do we need to win a war
  o Having a war reserve mode would be a good idea – adds uncertainty for the adversary
  o War mode must be given a great deal of protection
• There have been tabletop exercises over the last 20 years that have had elements of cyber warfare
  o When it appears, it generally stops the scenario
  o Stopping the scenario is not allowed, so go on without the cyber complications

Threat to the integrity of systems
• If I have had access to your system, and you know I have had access, you will always worry about its integrity – even if I did not do anything to that system
• Upsetting the integrity of a system may have the most damaging impact of all

DoD is not well organized to handle this problem
• Studies usually start out with the conclusion that DoD is not well organized for any given situation
• However, no one comes up with a really better way of organizing
  o Once all the elements are balanced and constraints are taken into account
• Gerstner’s book *Who Says Elephants Can't Dance?* is important here
  o Describes what he needed to do to end the death spiral at IBM
• One important element is that we can’t afford to have different elements of the national security community fighting each other over changes in the organization
• New DNI ADM Blair does have a deep understanding of the issues involve

It is possible to design systems where man-in-the-loop controls allow the overriding of some malfunctioning automated control, but it becomes increasingly difficult as more automated systems are being relied on