



Introduction

WHAT AUTHOR WANTS TO SAY

“START BY DOING WHAT IS NECESSARY,
THEN WHAT IS POSSIBLE, AND SUDDENLY
YOU ARE DOING THE IMPOSSIBLE”.

St FRANCIS OF ASSISI

A SHORT STORY

ONCE SOMEONE ASKED A FARMER “IF HE HAD SOWED WHEAT FOR THE SEASON”. THE FARMER REPLIED, “NO, I WAS AFRAID, IT WOULD NOT RAIN”. THE MAN ASKED, “DID YOU PLANT CORN”? THE FARMER SAID, “NO, I WAS AFRAID OF INSECTS EATING THE CORN”. THEN THE MAN ASKED, “WHAT DID YOU PLANT”? THE FARMER SAID, “NOTHING, I PLAYED IT SAFE”.

THAT'S WHERE WE ARE IN IW STRATEGIES

NEVERTHELESS,

LET US TAKE A STEP FORWARD

TO BEGIN OUR LONG JOURNEY TOWARDS

INFORMATION WARFARE.

In the early 1990s, as part of their preparation for Operation Desert Storm, U.S. forces deployed extensive data networks throughout the Middle East. The military came to rely heavily on these networks for logistics and support activities.

- When Desert Storm actually began, data traffic suddenly increased. The networks choked.
- Users in Saudi Arabia could not receive or transmit information.
- Fix would have to be done remotely as expert was not available locally.
- Fix was done remotely from US by connecting over the Internet. Not a secure connection to say the least!
- The problem was solved. Or was it?

Lessons Learned

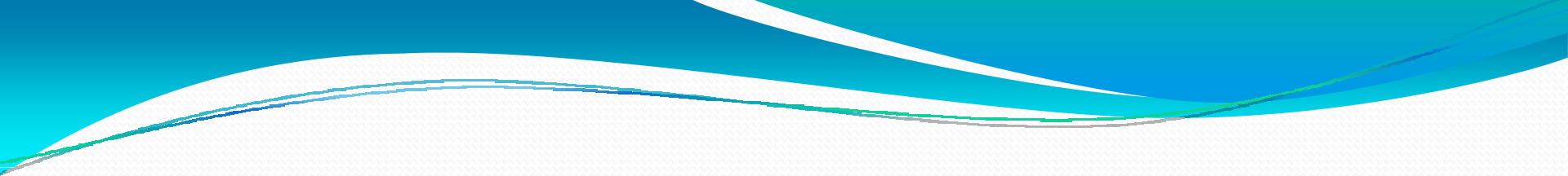
- **Lesson 1: Availability**. Troops in Saudi Arabia had the most sophisticated IT at their disposal, but were cut off from vital communications when they most needed it. If info was not available when it was needed, it was of no use.

- **Lesson 2: Confidentiality**. The problem was resolved, but it was fixed remotely via an insecure connection. If one of *ours* can access the system over the Internet, couldn't one of *theirs*?

- *"Computer hackers in China, including those working on behalf of the Chinese government and military, have penetrated deeply into the information systems of US companies, electricity grids and government agencies....."*
- National Security Advisor M K Narayanan, in an interview, told The Times that his office and other government departments were targeted on December 15, 2009.
- *Major countries and nation-states are engaged in a "Cyber Cold War," amassing "cyber weapons," conducting espionage, and testing networks in preparation for using the Internet to conduct war....*
- Google Inc's threat to quit China over cyber attacks and censorship highlights U.S. fears that a more powerful Beijing is tapping government and corporate computer networks to steal secrets and to prepare for potential conflicts.



Foundation of Strong Net-Centric Operation

- 
- A robustly networked force improves information sharing.
 - Information sharing and collaboration enhance the quality of information and shared situational awareness.
 - Shared situational awareness enables self-synchronisation.
 - These, in turn, dramatically increase mission effectiveness.
 - Here ‘synchronisation’ may be viewed as the coordination and orchestration of operation so that they occur at the desired time and place.



Challenges Before us

Technological:

- Virtualisation and automation
- *Mobile computing*
- Cloud computing
- Collaborative developments
- Global class competition

Business Environment:

- Hyper-connected world
- Unstructured Internet Infrastructure
- Collaboration









































Behavioral:

- Increased comfort with outsourcing
- *Social networking*
- Consumerization of IT
- Self service
- Rigid mindset - Easy money, cyber terrorism

Business Requirement:

- Reduce cost of solution
- Accelerate response time
- Simplify, Ease of use

Key Flaws in Existing Technology

- Network security technology operates with **virtually no knowledge about what it's protecting**
- Virtually all network security technology is **driven solely by different product vendors** without any collaboration and standardization
- These factors combine to lead to **network defenses that are misconfigured, porous, and static.**



Impact

• The world's increasing reliance on information technology, combined with the growing sophistication of cybercriminals and cyber attacks, is leading to a sort of cyber-cold war.

• The very nature of the Internet lays countries open to cyber espionage and cyber war. "Networks are more open and porous than before, and that makes attacks easier".

Example of a Destructive Collaboration

Los Angeles Times
latimes.com
April 16, 2007

A World Wide Web of terrorist plotting

The Internet has become a virtual operations center replacing the Al Qaeda bases in Afghanistan and Bosnia.

By Sebastian Rotella, Times Staff Writer



Bektasevic, 19, stands in court in January, when he was sentenced to 15 years

SARAJEVO,
BOSNIA-
HERZEGOVINA

They never met face to face, but the two young zealots became brother warriors in the new land of

than Arabic and listened to the rap of Kanye West along with the harangues of Abu Musab Zarqawi. Their Western ways enabled them to communicate and cross borders with ease. And investigators say they had a youthful disregard for life.

At the same time, many were amateurish and reckless. That made them easier to track, but presented investigators with a dilemma: A fighter may lack experience, but he remains a menace if

VOCs do exist

VOCs can be very effective

They never met face to face, but the two young zealots became brother warriors in the new land of jihad: the internet



Accepting the Challenge...



The threat can effectively be challenged and contained by a strong net-centric operation. This would need

- Some amount of restructuring of Internet
- This will be a very expensive proposition, but the cost could be shared among governments, private companies and individuals. The cost of security now is enormous, with people losing billions of dollars, and governments having national security compromised because of this.
- CII Can play a significant role in bringing the stakeholders together and building a strong nation



Conclusion

EVEN THOUGH:-

- The awareness of the problem is there
- Billions of dollars have been spent on IT security

STILL:-

- The security problem is getting worse as attackers become more motivated.

How is it possible for so many security technologies to be defeated?

SHOULD WE NOT CONCLUDE?

- The silo approach of “see a threat, buy a box” is no longer feasible. We need to be collaborative and beyond the sense of material gain.



Thank You