CYBER DOMAIN SECURITY

An 'Outside the Box' think for a different future

Michael W. Wynne
21st Secretary, United States Air Force
October 17, 2017

Cyber Domain Security

The Promise of Cyber was for a better future in Command, Control and Communications

The Vulnerability of Cyber returns C3 to the yesteryear Electronic Warfare on Steroids

As Hill Street Blues would script:

'Let's do it to them before they do it to us'

Cyber Domain Security

What I want to communicate today

We Understand the Physics and Constraints of the Physical Domains?

- Laws, Agreements, and Mutual Enforcement
- Clear Image of Good and Bad Enforcement by Policing or Military action

Today we are struggling with Vulnerability of the Virtual Domain—Cyber?

- Technology created a comfortable user friendly seemingly easy environment
- Bad Actors and Malevolent Designs meet each convenience with Bad outcomes
- How to assess: If this is a giant false start, and can technology solve the problem?

If a False Start, can Military/Civilian muster the discipline to correct

Cyber Domain Security

Old	Replacement
Horses	Automobiles, Buses
Industrial Manpower	Mechanical Revolution
Mechanical Revolution	Electric Power
Vulnerable Circuit Design	Hardened Circuit design
Wired Telephone System	Cellular System
Regular Cellular	Smart Phones
Tubes and Gears	Integrated Circuit-Turing
Integrated Circuits-Turing	**?**

Cyber Domain Security

To Think 'Outside the Box'

Need Agreement on the issue

First: A: Examine whether the basis of Our Digital Networks (Turing Machines) need to be replaced

B. Do Software corrective actions suffice

Second: Examine the Barriers to effect a true solution

Third: Prioritize the Pressing Applications to begin

Hackproof Technologies, Inc – All Rights Reserved

Cyber Domain Security

Thesis: **TURING Computer Security is Impossible**

Sony Root Kit
"Ignore me"

"This Sentence Is False"

Stack Overflow
"Do This"

Malware Goes Here

Self-Deception Goes Here

If it's true then it must be false, so
Assert it false, and infer that it is true so
Assert it true, then it is false, but …

General Recursive ISAs Loop Forever

Proof: Gödel-Kleene: 1934: Halting Problem Identified

Thus: Hack the Policy Reasoner

© 2017 Hackproof Technologies, Inc All Rights Reserved

CYBER DOMAIN SECURITY

Early Warning Signs About the issue

Pranks and Learning to Hack

- Incident in College Library deleting files not saved
- Defacing informational sites
- Diversion of searches

US Government cites the issue

- Condoleeza Rice talks on www as wild wild west, with duping of ordinary users
- Unannounced Break-ins to data files leads to firewalls and encryption
- The US Air Force Mission altered to include the Cyber Domain

Dire warnings up to present

- Loss of critical or Intellectual Data Files, Property
- Concerns about national attacks on infrastructure
- Cities, Health Care providers, Movie Studios files taken for Ransom

CYBER DOMAIN SECURITY

Signs of an Issue: Growth of Private Armies

Establishment of Public and private protection

- Unannounced Government Universities
- Announced College Training and learning
- Growth of web based 'protectors'
- Industry revenues top 20 Billion, and more

Spy versus Spy erupts

- Contests on Hacking
- Rise of 'Black Hat' convention, Hackers as teachers
- Platforms at risk-Autonomous Vehicles, some C3I, some Offensive

How Much Protection is enough

- Legislators pass laws to protect public—not possible—Active Forensics?
- Industry Operators ask for guidance –what do we do? Resilience?
- Gate Guards, and Mal-detectors is cited as sufficient legal protection

Cyber Domain Security

Signs of an Issue: Society's response to Cyber Security

Ambivalence because of loss of control

- We lock our doors, and cars, but follow instructions for IT security
- We look to Providers to set up protections
- Providers look to lawyers for liability relief

Efficiency is higher in order of needs than security

- When security has requirements, employees complain about impact on work
- Consumer convenience and belief in anonymity

Business/Military becoming more not less dependent on Cyber Security

- Movement to cloud, fusion, long range control
- Introduction of remote monitoring with after action audit to reduce costs
- IT upgrades focus on productivity, with security as a stated benefit
- Security maintenance for Mal-ware is a booming segment, post impact analysis

Cyber Domain Security

Signs of Issue: Society's response to Cyber Security

Shaken Belief That Nations security service is the best

- Shaken by Hacking of Government entities—is hope a strategy?
- Corporations do not go public with loss
- Banks mark up for losses as cost of business

Solutions Offered for Impact on daily lives

- Life Lock offers ID Protection
- OPM offered subscription to Insurance for impact
- Life goes on, both on line and physically; lot's of targets, little impact

Free Capitalist Society, does not see solution just ahead

- Lot's of adverts on advanced protection—Guarantees?
- A belief that one can pay for protection if needed
- Only in tight circle does NIST warning about **impossibility** and its impact

Cyber Domain Security

Signs of an Issue: Long Term Impact on Society

Transfer to Start –up industries

- Cyber Theft first traceable to woolen mills using photographic memory
- Cyber Theft of Intellectual Property allows competition catch up—Pol/Mil
- Impact is loss of Economic and Military Margins

Lack of Innovation

- Discouraged producers might produce less innovation
- Impact of theft creates second class industry, harder to remain dominant
- All of world society loses in cyber open season

Emphasis grows on encryption and coding so minimize gains

- Last years fight over Apple Phone a harbinger of the future
- Clouds response is to encrypt and scatter data around multiple service centers
- Emergence of multiple media authentication—once reserved for spies

Cyber Domain Security

Societal Actions required: The Enemy Gets a Vote

Cyber Gang Tactics are changing

- Phishing going mainstream
- Never open an external file
- Insider Failures lead to 'ransom-ware'
- Insurance Companies are resisting costly policies, pushing protection

National Level Cyber are changing

- Cataloguing unprotected sites, 'white listing' as gate keepers
- Leaving Sophisticated Advanced Persistent Code behind
- Targeting Infrastructure rather than just Command and Control Centers

Combining Physical and Virtual Combat Forces

- Fully integrating cyber into combat profile
- Keeping what helps and discarding difficult targets
- Keeping Intel open to Cyber Capability of opposing forces

Cyber Domain Security

Pause for **Observations: Where to go from here?**

World Future in Cyber

- Cooperation or Conflict
- Innovation or Stagnation
- Protect or Remain Vulnerable

Current situation

- Systems are set for productivity
- Convenience is compromised by Security
- Current Level of turbulence is tolerated, expected, exposing Civilian Infrastructure Economy to essentially military action, no retribution—bigger walls, deeper moats– counter Military Action?

Future Desired State

- Retention of productivity and convenience
- Security is embedded, and systems are self checking
- Attack and Defensive force applications are returned to physical sciences, retaining protected Command and Control. Husbanding advantages to our own development.

Cyber Domain Security

Pause For Observation: Where to go from Here?

Twelve Step Program brought by Alcoholics Anonymous

- Stipulates that behavior change must start with admission of problem
- Included is a stipulation that a solution is present and must be pursued
- Determination and Discipline are required

We have been involved in digital computing since 1930's

- Though considered academic, by mid-1940's large digital processors were in test
- These large scale processors were driven by analog elements, to accomplish digital outcomes
- The discovery of integrated circuits began to eliminate analog from designs

Systems design has a base requirement to measure responses to all inputs to the system

- The emergence of totally digital systems forgave this violation of responses
- Beta testing and cycle of corrective action minimized self induced 'Bugs'
- The inter-connection of digital systems allowed for externally induced 'Bugs'

Cyber Domain Security

Where Is Society Relative to Issue of False Start?

Society believes there is a problem

- Presidential Level Direction to resolve
- Broadcasts when major attacks occur
- Insurance Conferences are littered with Cyber Intrusions

Legislators are discussing freedom and protection

- As early as March/April 2001, FBI acknowledged problem
- Military Services cited concerns in 2006, began to organize
- Few hearings in our congress do not involve Cyber Issues

Cyber Conferences are every where, even here

- Stevens Institute held wide ranging conference in Washington back in 2010
- There was, and still is worry and concern, detection and correction, whole network is in BETA test, looking for 'Bugs'—now called Mal-Ware
- Cyber Industry now nearing $20 Billion and growing—Band Aids, or fixes?

Cyber Domain Security

Where to go from Here?: Systems Engineering Principles

There are high level principles

- Build the Right Systems and build the system right
- Do the right things and do the things right

There are more specific principles

- Base the Development Cycle on removing risk and enhancing value
- Specifications flow up as well as down the architecture
- Decompose systems, not requirements

There are base Principles

- For a system, every output response should be linked to an input
- For a system, there should be a finiteness to the possibilities of output signals given a known finite set of possible inputs
- The possibility of Garbage In; Garbage out is eliminated-corrected
- Externally induced inputs differing from known inputs are rejected

Cyber Domain Security

Personal Experiences

Working with Mechanical and Analog Systems

- Infrastructure largely consists of aging Mechanical Systems
- Manufacturing applications are fine applications of mechanical/ analog
- Because they are electrically controlled, managing by observation was the rule

Working in the pre-connected IT Space

- Broke a large computational system by overwriting the executive routine
- In controlling air surfaces with a Computer, put a random table access in control loop
- During a test of and educational system a smart colleague discovered no firewall between stored and random memory, forced shutdown

Observation on Working in the connected IT space

- Mistakes, once called 'Bugs' and 'Glitches' now deliberate Mal Ware
- 'Bugs' and 'Glitches' naming reserved for development cycle, not operational
- Systems design seems to target development cycle, integration, as discipline no longer know for all possible inputs (finite, countable) there are known outputs

Cyber Domain Security

A Technology Resolution:

Applying the concepts of Systems Engineering Holds out a path for a different future

- Finding a Turing machine substitute
- Requiring Defined outputs for every input
- Effectively requiring corrections for 'Bugs'; 'Glitches' and 'Malware'
- Restoring Operator Authority and Control
- Hardening Circuits to EMP or Power Infrastructure Surge
- Retaining Convenience and Productivity wherever possible

Cyber Domain Security

A Technology Resolution:

Applying the concepts of Systems Engineering Holds out a path for a different future

- This effectively restores problems to development, ending public issues of detection
- This nullifies the effect of 'distant disruption', hardens against Physical response
- This can retain the value of Cyber, but reduce Military and Societal Issues, through research
- Works in combination with Encryption for Privacy

Cyber Domain Security

Is there such a device?

We have together tracked the history of the **Integrated Circuit**, seen how it has grown smaller, yet more Powerful

We have not tracked its counterpart in finite arrays–
the **Fully Programmable Gate Array** (FPGA) Technology

Finite Gate Arrays conform to the principals of Systems Engineering – measured, bounded, proven hardening techniques

They have as well taken full advantage of the technology revolution of Small yet more powerful, fit into server board slots, can be on the Internet

They only process as planned, requiring offline, physical updating

Cyber Domain Security

Where to go from Here?

Thus Far we have travelled a path illustrated by the twelve steps

- We have Highlighted a Military and Societal issue
- We have identified where we possibly took a wrong path
- We have essentially proven, both theory and practice that it is the wrong path
- Now we must evaluate possible corrective actions

Do we have the discipline to restore the benefit while correcting the deficiency?

- Where to start?
- Can we prioritize the substitution set?
- When are we completed?

Can Start with Call to Action

Cyber Domain Security

- Today the **IC Turing Circuit Board** hardware is dirt cheap and available as a plug in to any server; while the value is in the app that runs upon layers of software with myriad vulnerabilities.
- Tomorrow; the **FPGA Board** hardware, will be less expensive to own and operate, also as a plug in to any server. With no more layers of vulnerability. It will require more careful coding in the initial set-up, with integrated apps.
- In both scenarios **Disciplined User Policies** will still need rigor to insure no misuse; but once the FPGA is installed, like a mechanical gear, maintenance should be low.
- Such a Transition will take prioritization and determination —
  such is the essence of **Systems Engineering Discipline and Control**

Cyber Domain Security

Where to go from Here

With Known Solution

- Apply to Military Weapons, and Command and Control Systems
- Apply to Public Utilities, Electric Grid, Gas
- Ultimate Goal: replace 'Turing' enterprise, retaining advantages

Prioritize: Yes

- This will squeeze out the Gangs, and 'Mal Ware' from Bad actors
- This will not correct development errors, but will allow correction
- Military and Civil is now at risk, therefore next move is to protect

Cyber Domain Security

Summary

This Cyber domain is one of vulnerable convenience, operating a society or a military does not anticipate malevolent action, absent ability to police

The Enemy, either Nation States, or bad Operators is voting every day to make things worse

Corrective Action starts the **Hardware revolution**, and possible reduction in software dominance

First mover can have an **enormous advantage: Both in Civil and Military applications**

Can be done but will take disciplined action

Mirrors the change from Industrial to Electric

Thank You

For allowing me to Talk of this Very Different Look at Cyber
With strong leadership; We can make this different Secure future a reality

Cyber Domain Security

Sources

1. R.L. Dick, FBI, Testimony 4/3/01
2. AP News 3/24/16 T. Abdullah and E. Tucker
3. a. AP News 3/24/16 Abdullah and Tucker

   b. IBT World: Russia- NATO Cyber 10/14/15 C, Harris
4. WebSphere Journal 3/18/06 Six Principles of Systems Eng. M. Cantor. G. Roose

5 Recent Articles by Wynne, 11/2016 "It's the Hardware Stupid"; "Paying Protection to the Wrong Gang"; "Really Protecting Democracy—with Analog Computing" www.SLDinfo.com.