



# Cyberspace as the 5<sup>th</sup> Domain of Warfare

Linton Wells II

Centre of Excellence for National Security (CENS)

Distinguished Visitor Program (DVP) Lecture



© 2016



# Overview

- Domains (dimensions) of warfare
- Often-conflicting concerns & challenges to concepts
- Velocity of tech change
- Cyber attack chain and decision cycles
- Cybersecurity and mission assurance
- Cyber-EW convergence
- Converging public-private components
- DEF CON observations
- Real world example: Ukraine
- Organize, train and equip
- Next steps

# Domains of Warfare

- Land



- Sea



- Air



- Space



- Cyberspace



Question: is cyber a domain of warfare, or of war?

# Often-Conflicting Concerns

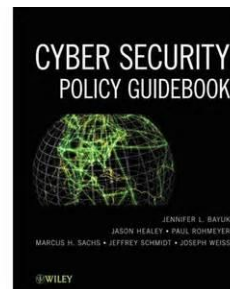
- Offence vs Defence



- Civilian vs. Military



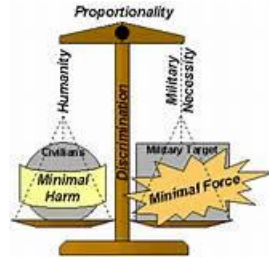
- Technology vs. Policy





# Challenges to Traditional Concepts of War

- Proportionality, attribution, mutually assured destruction



- State vs. non-state actors



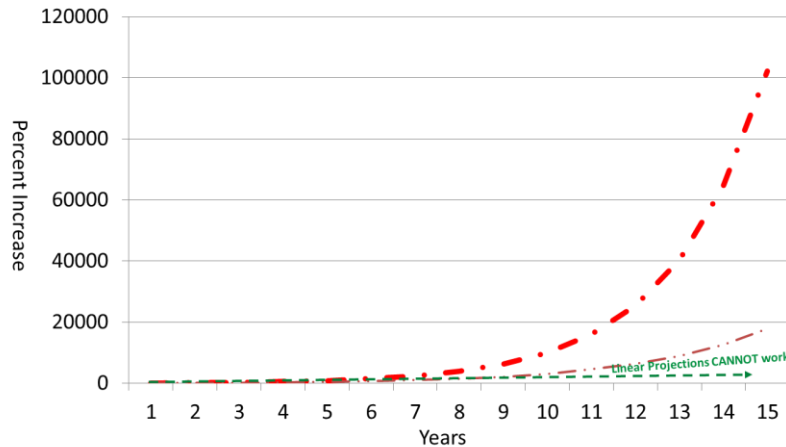
- Military vs. dual use infrastructures



# Velocity of Tech Change

If a factor, e.g. computing power/unit cost, doubles every 18 mo, 5 yr increase is 900%, 10 yr 10,000%, by 2030 ~100,000%

Growth in Computing Power per Unit Cost



Capability doubles every 18 months — · — · —      Capability doubles every 24 months — · · · —

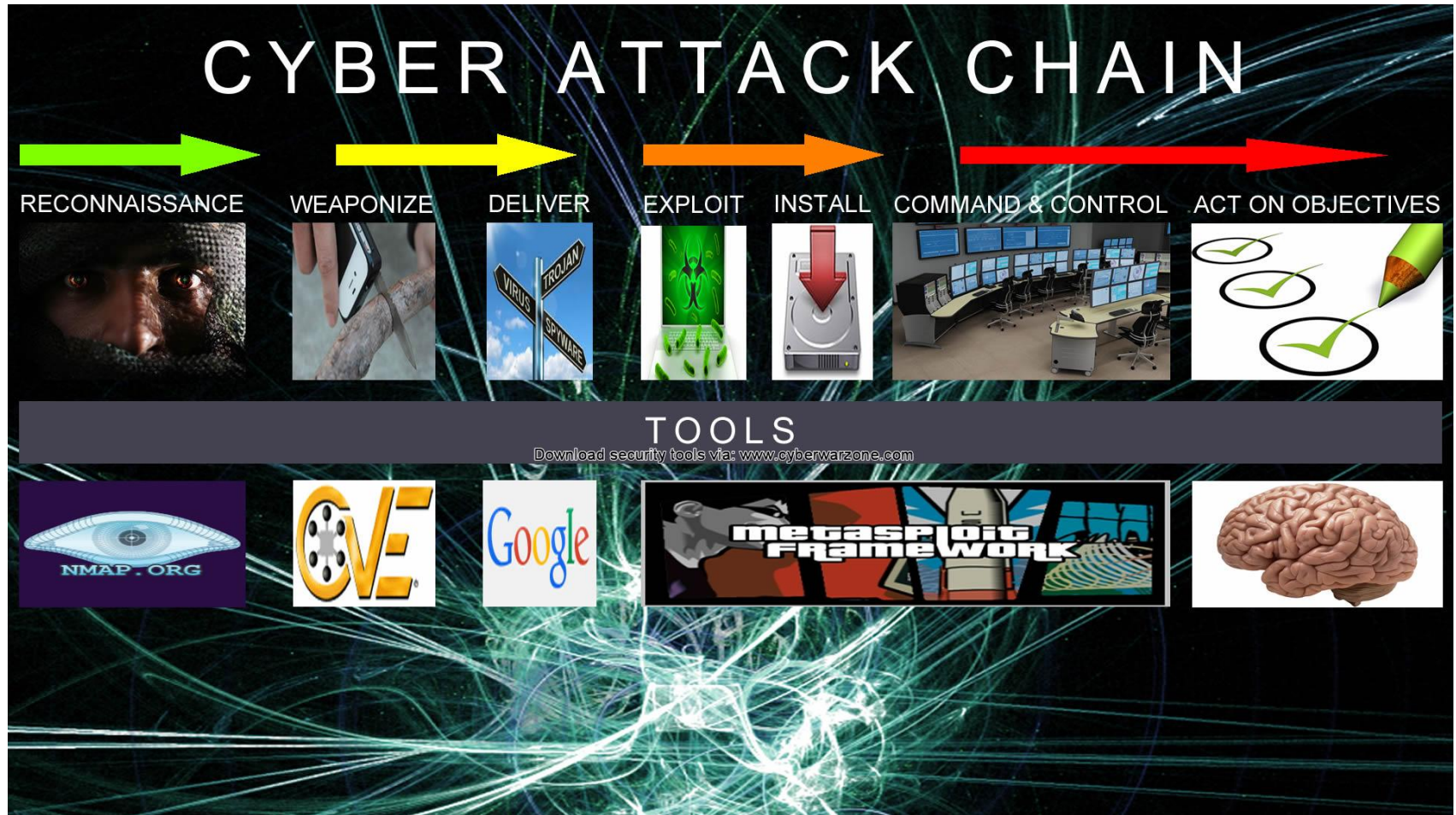
Biotech even faster, robotics ubiquitous, nano poised breakout, energy impacts are global

- Think BRINE (bio-robo-info-nano-energy) + Additive Manufacturing

Interactions complicate things

Linear projections CAN'T work

# Cyber Attack Chain



cyberwarzone.com

# OODA Loop & Decision Cycles

- “Observe” and “Orient” phases increasingly electromagnetic
- “Decide” and “Act” supported by information processing
- Cyber can dominate OODA loop in all domains
- Tech changes
  - Processing power
  - Machine learning
  - Sensor proliferation
  - Army 2050 battlefield—can you move?
- Speed of decisions
  - “Man-on-the-loop,” vice “Man-in-the-loop”



Image courtesy [successing.com](http://successing.com)



# Cybersecurity and Info Sharing

- Confidentiality, Integrity, Availability
- Perimeter defenses insufficient
- Alternative approaches to cybersecurity
  - Big data
  - Near-Real Time anomaly detection
  - Supply chain, blockchain
- Major policy, legal, moral, ethical, privacy issues

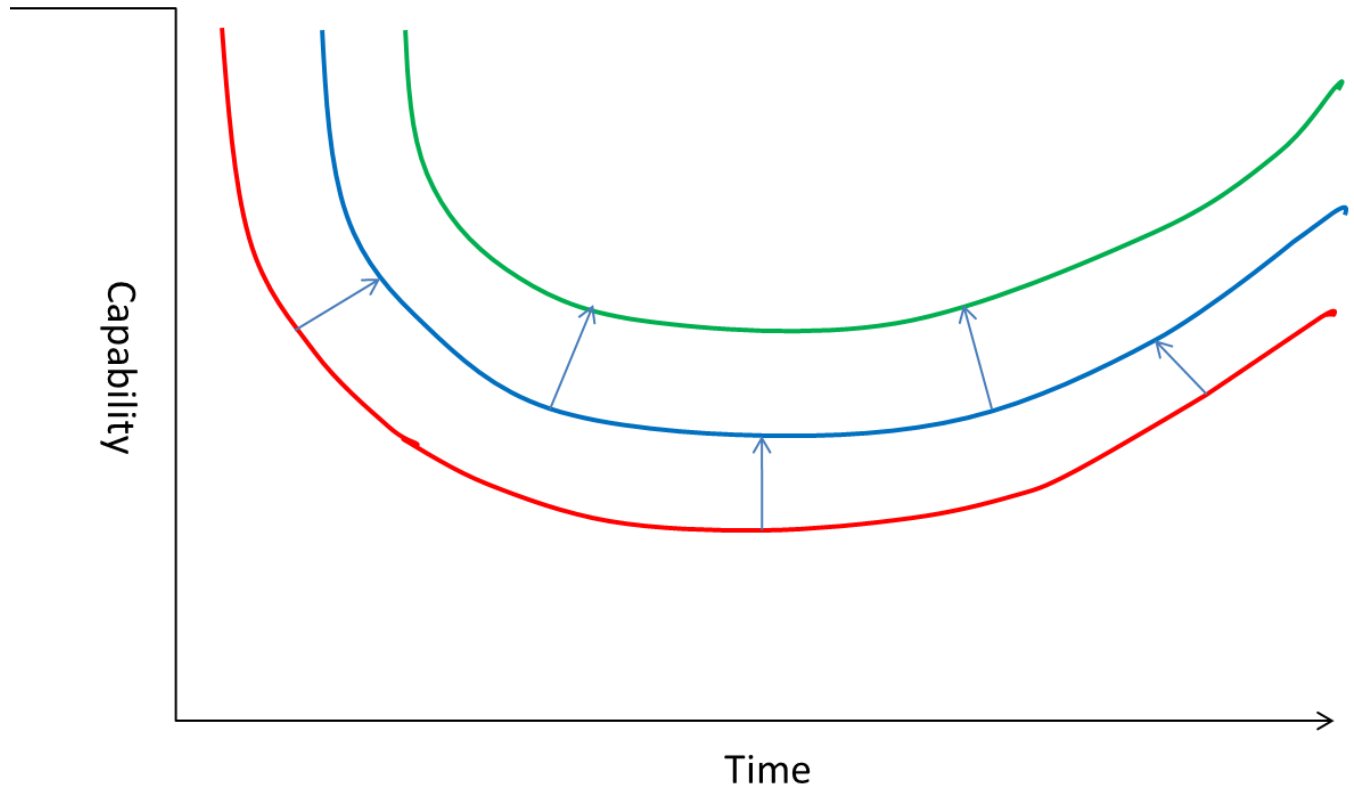




# Mission Assurance

## Restoration of Capability

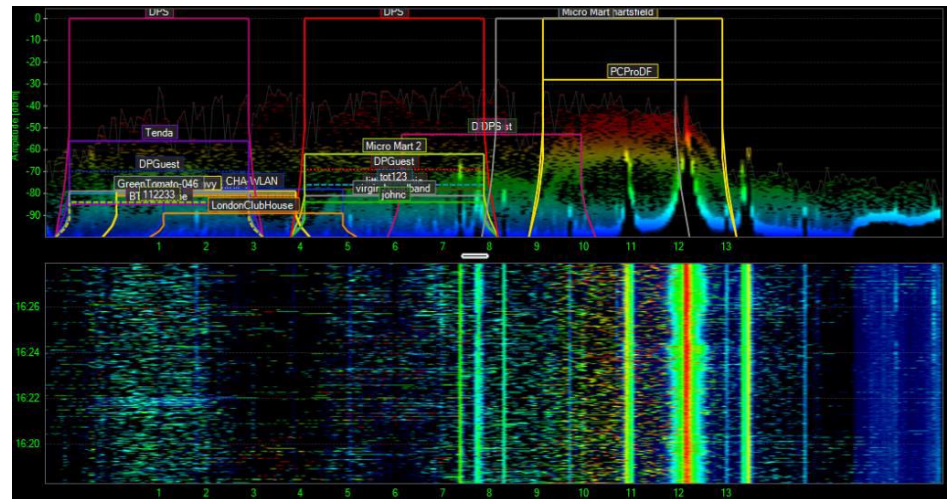
Goal is to build resilience to make “the bathtub” as narrow and shallow as possible



# Cyber and EW Convergence

## Kinetic & Non-Kinetic Fires

- Maneuver in Electromagnetic Spectrum (EMS) Space
  - Navy Electromagnetic Maneuver Warfare (EMW)
  - Army Cyber Electromagnetic Activities (CEMA)
    - EW Planning & Management Tool (EWPMT)
  - Marine Corps Cyber EW Coordination Cell (CEWCC)
  - USAF
- C4ISR Implications



# Third Offset Strategy


## [3<sup>rd</sup> OS] (1)

- Leverages many similar technologies as 4IR
- Focused on challenges like:
  - “1,000 nautical mile anti-access challenge...
  - Inter-theater area denial
  - Closing the last tactical mile,
  - All while operating under intense cyber & electronic warfare attacks”

All quotes from DepSecDef Robert Work 2015

Infographic from Avascent Analytics, <http://www.avascent.com>

8/31/16 final linwells@gmail.com, 202.436.6354, Skype: linwells



## THE INNER-WORKINGS OF THE THIRD OFFSET

First Offset (50s)  
Nuclear Advantage

Second Offset (70s/80s)  
Precision Strike

### AN ENDURING DEFENSE PARADIGM

**TWO TRACKS**

Short Term (3-5 years)  
Rapid Prototyping

Long Term (10-20 years)  
S&T


Breakthrough technology or novel use of existing technology


Speed first, in combat & acquisition


*"We have a resurgent Russia and a rising China. We need to focus on these high-end adversaries."*


- DEPSECDEF Robert Work


### KEY ELEMENTS


  
Autonomy & AI


  
Guided Munitions

  
Submarine & Undersea

  
A2/AD

  
Space

  
Cyber/EW



- 1 ENGAGE CUSTOMERS**

RESET LAB RELATIONSHIPS  
BUILD RELATIONSHIPS WITH NEW ENTITIES  
ASSESS CUSTOMER GAPS
- 2 SHAPE OPPORTUNITIES**

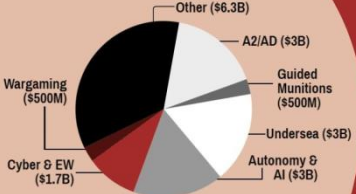
LAB TODAY, ACAT I TOMORROW  
INFLUENCE EMERGING REQUIREMENTS  
ADOPT RAPID PROTOTYPING MINDSET
- 3 ALIGN CAPABILITIES**

REVIEW INTERNAL GAPS  
ASSESS NEAR-TERM FEASIBILITY  
PLAN FOR STRATEGIC INVESTMENTS
- 4 IDENTIFY PARTNERS**

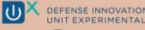
AMPLIFY CAPABILITIES  
ADDRESS GAPS  
CONSIDER SILICON VALLEY, FFRDCS, UNIVERSITIES
- 5 EMBRACE EXPERIMENTATION**


FUNDS ARE BEING DISPENSED NOW  
HAVE AN EXPERIMENTAL MINDSET  
EXPLORE INTERNAL DISRUPTION


**\$18B OVER FYDP**  
to be allocated to the Third Offset (FY17 Budget Request)




### KEY ORGANIZATIONS

  
DEFENSE INNOVATION UNIT EXPERIMENTAL

  
Strategic Capabilities Office

  
ARL

  
DARPA

*"The Third Offset is simple. At its core AI and autonomy will lead to a new era of human-machine collaboration."*

- DEPSECDEF Robert Work



# Third Offset Strategy (2)

- 5 main building blocks:

- Learning machines:



- Human-machine collaboration:



- Advanced human-machine combat teaming:



- Assisted human operations:



- Autonomous weapons:

- Able to withstand cyber & EW attacks



Focused on potential adversary **capabilities**, not just intentions

# Third Offset Strategy (3) & Cyber

- Goal of 3<sup>rd</sup> OS is to “make humans more effective in combat” Much in common with 4th Industrial Revolution
  - In both areas people must be empowered to address most serious challenges
  - Tech is important, but both involve adaption and, ideally anticipation, across organizations, people, and processes, as well as technology
  - Cyber is integral to virtually aspects of the 3<sup>rd</sup> OS
- **NOT JUST TECH**

# Commercial Convergence-- Sensors

- Open Source ISR-GIS



- UASs



- IV4 (Info Volume, Velocity, Veracity, Value)



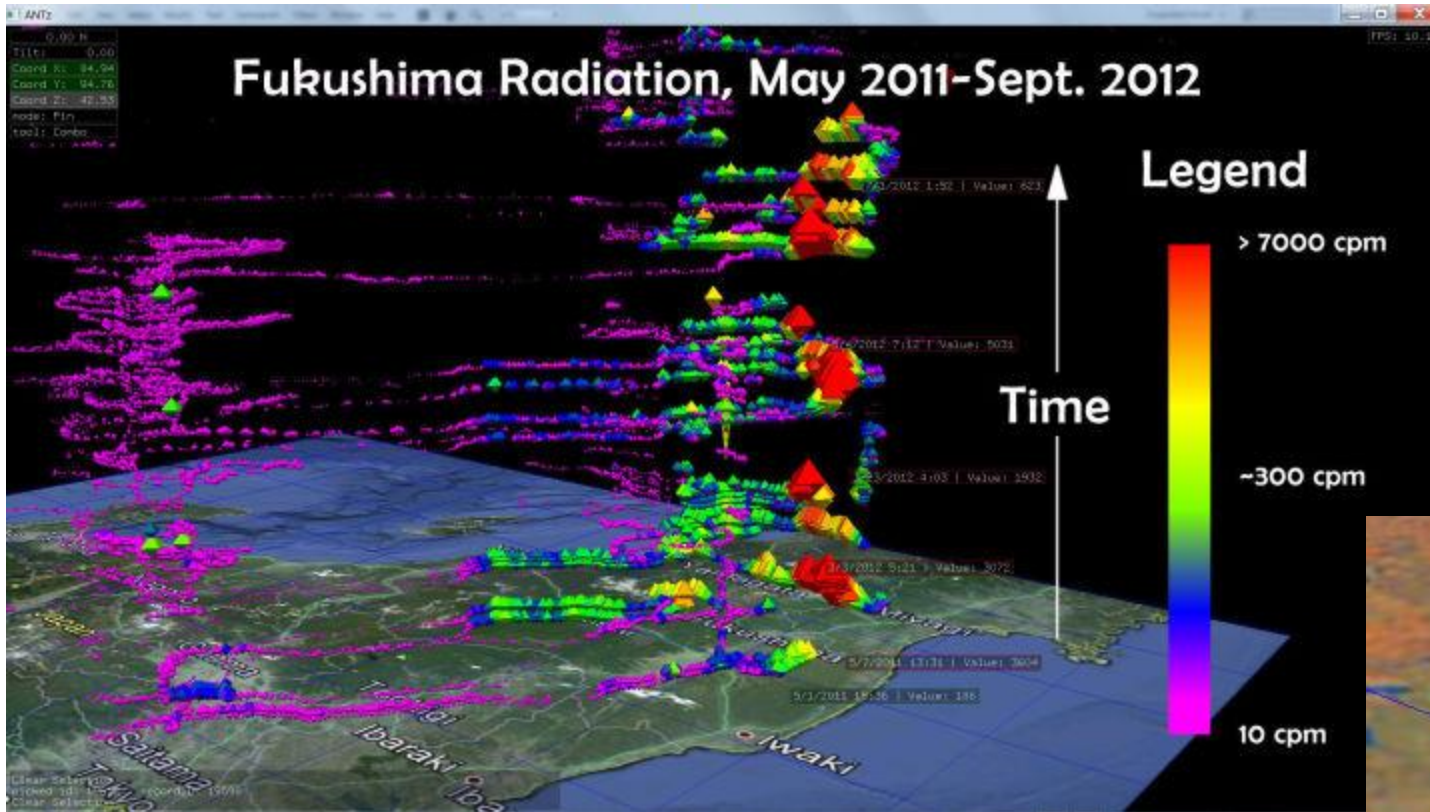
- Mobile, Wearable



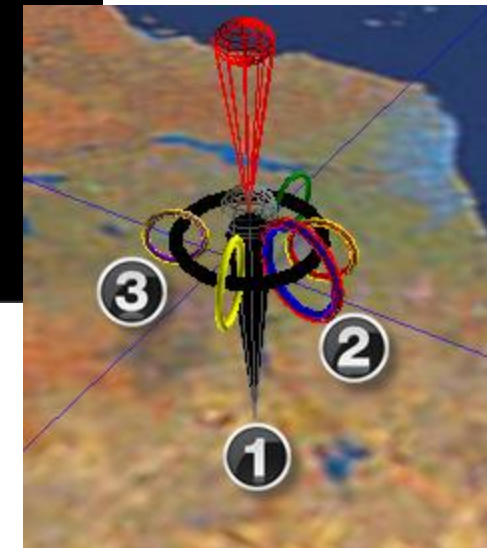
- Internet of Things (IoT)



# Commercial Convergence-Displays



Graphics by SynglyphX





# DEF CON 2016 Observations

- **No reason for complacency** about cybersecurity, or even much optimism, but DARPA's **Cyber Grand Challenge** (CGC) was new:
  - Artificial Intelligence (**AI**) and Machine Learning (**ML**), plus
  - Focus on security operations at the **binary level** and
  - “formal verification” of code, offer ways to
  - **“imagine a future with some likelihood of cybersecurity”**
- **Speed**: Emphasized repeatedly, e.g. reducing Time to Detect (TTD) malware, remediating flaws faster, and aggressively updating code.
- **Infrastructure remains vulnerable**, complicated by weaknesses in the Internet of Things (**IoT**)
- Software Defined Radios (SDR) and Software Defined Networks (SDN) can be secured, but
  - they require people who can **integrate hardware and software** fixes, and **very skilled systems administrators**.

# The Humanitarian Side of Cyber

Categories of Humanitarian Activities, Definitions of Cyberspace Operations  
And How They Might Apply to Humanitarian Environments



Prepare



Cyberspace Operations



Respond



Peace  
Operations



ICRC

International Humanitarian Law

8/31/16 final

linwells@gmail.com, 202.436.6354, Skype: linwells

# Cyberspace Operations and Humanitarian Operations

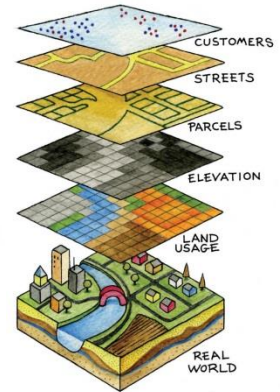


Comms, Lift & Power



Diverse Components

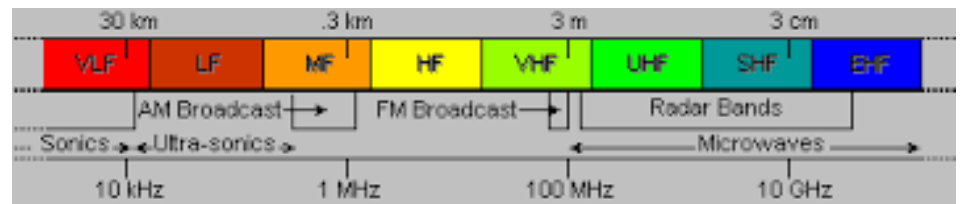
IV4



Geospatial Information Systems (GIS)



Deny, Disrupt, Degrade, Destroy, Deceive



RF Spectrum for Comms



# Netwar\*

- Cyberwar is “...the act of disrupting, if not destroying, information and communication systems ...on which an adversary relies in order to know itself...”
- in Netwar the actors seek to “...disrupt, damage, or modify what a target population knows or thinks it knows about the world around it.”
- Plays directly to increasing challenges of IV4 since it
  - Involves “deliberate combinations of diplomacy, propaganda and manipulation of media”
  - Russians are using masterfully
  - “Fortunately, the antidote to Netwar is active transparency, a function democracies excel in.”
- “...Cyberwar and Netwar have become increasingly intertwined, and the impact of Cyber actions can be either potentiated or mitigated by corresponding psychological and normative conditions. Thus, an effective cyber defense must also have a set of informed Netwar responses.”
- Netwar concepts also apply to humanitarian activities

\* Robert Brose, “Cyber War, Netwar and the Future of Cyberdefense,”



# Real World Example—Ukraine\*



## Chronology:

- 2012 Computer defacement
- 2013 Advanced malware deployment
- 2014 Coordinated hack against national election, 25 May 2014.
  - Influence election and integrity of data.
  - Russia TV announced winner as being far right
- Christmas 2015. Electricity grid attack.
  - Very coordinated. Most sophisticated attack yet. Excellent timing, creativity
- Not one-way: Electronic billboards hacked in RU by Ukraine
- Social media story--follows Ru soldier from home in E Ru into Ukraine and back—undercuts RU denials
- Fire in Odessa. False Facebook account. IO effort.
- Journalist in Ukraine killed in car bombing, July 2016

\*Kenneth Geers, "Cyber War in Perspective. Russian Aggression against Ukraine" Briefing at black hat 2016

# Ukraine (2)

- **How Russia uses false stories to shock and paralyze international dialogue:**
  - The war for “reality” as world is increasingly connected—Russia is perhaps busier than any other nation in planting inflammatory rumors and sensational stories via the internet that get picked up by sites like Sputnik and RT.com.
  - The problem has become so bad for West that “that both NATO and EU have established special offices to identify and refute disinformation, particularly claims from Russia.”
  - “The fundamental purpose of dezinformatsiya, or Russian disinformation, experts said, is to undermine the official version of events — even the very idea that there is a true version of events — and foster a kind of policy paralysis.”

(Neil MacFarquhar, *New York Times*, Aug 28, 2016, *A Powerful Russian Weapon: The Spread of False Stories*)

- **Basic Russian IW message:**
  - “Russia is a misunderstood and misjudged superpower, and a necessary counterweight to Western liberal values. By contrast, the West has experienced a decay of ‘traditional values’ and acts hypocritically in the international arena. As a result, the West’s philosophy, systems, and actions should not be trusted.”
  - In sum, the traditional ‘fog of war’ has changed in the internet era

(Margarita Levin Jaitner, “Russian Information Warfare: Lessons from Ukraine”)

# “War” in Information Space

## The Informational Environment Does Not Support War, It Is War

- “Merely restoring our technological edge will prove insufficient unless this catch-up is successfully translated into purposeful grand strategy”
  - Address both general, wide-ranging geopolitical uncertainty and
  - More specific regional security threats, plus
  - increased threats posed by increasingly technology-empowered non-state actors.
- Operational transformation based on speed, precision, knowledge and jointness may yield “a truly exquisite military machine”
  - “However that machine will not necessarily be able to overcome strategic mistakes and generate success. In other words, transformation of the U.S. military cannot replace strategy.”
- Logic dictates that we base the foundation of such a strategy on mastering the Information Environment....”

Edward J. Horres, “Towards a Fourth Offset Strategy,” <http://smallwarsjournal.com/jrnl/art/towards-a-fourth-offset-strategy>

# Organize, Train, Equip (1)

- Non-traditional missions
- Rapidly changing equipment
- Personnel skills in high demand by private sector
- Need multi-tiered training: leaders, techs, workers
- Difficult policy, ethical, and moral questions
- Many legal issues—ambiguities in applying Law of Armed Conflict to cyberspace
- No “rules of the road” for cyberespionage
  - Can only be addressed through bi-lateral and multi-lateral negotiations



# Organize, Train, Equip (2)

- Cyber capabilities **cut across domains**
  - Most techs don't look for cyber causes
  - Operating at policy-technology-sociology interface
- Cyber-EW **convergence** adds further complexity
  - Doctrinal differences, analog-digital equipment, etc.
- Conflicting exercise objectives
- Cyberspace operations lend themselves to **hybrid** (gray area) warfare
  - **Cyber-on-cyber alone is rarely most effective**

# Enhancing Collaboration for Cyber Defense

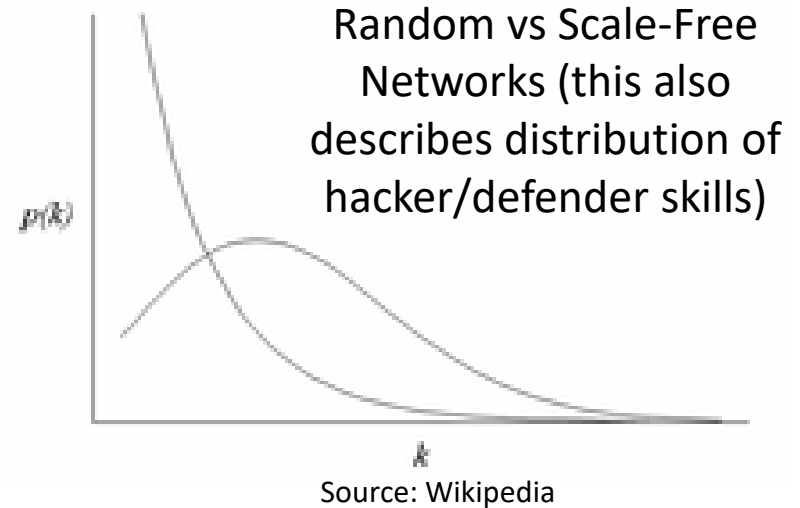
- Share threat data
  - Within govt, public-private, govt-to-govt
- Must collect meaningful data
  - And protect it
  - As tech evolves
- Focus on Mission Assurance
  - Build resilient, agile systems operating behind multi-tiered defenses

# Public-Private

- **Help private sector develop means** to respond to attacks
  - Not clear “privateering” analogy works
- Problems with ISACs (Information Sharing and Analysis Centers)
  - Now ISAOs
  - How to build trust
- Need better ways to assess and allocate risk in **public-private partnerships**

# Next Steps

- True talent is scarce
- Recognize top group
- AI & Machine Learning
  - Bridge training shortfall
  - Focus on binaries
  - Train (at high end) in autonomy/counter-autonomy
- Big data analytics
- New personnel policies
- OT-IT intersections



# Implications for Research

- Increased use of **dual use technologies** lend themselves to use by Alliance & coalition forces, using either secured networks or internet
  - Most don't involve controlled technologies
  - Exercise can examine minimum essential secure comms (thin line)
  - Tie to cyber ranges and training transformation
- Promote changes in how **organizations, people, processes and technology come together**
  - Link security and sustainability goals, public-private, trans-national mechanisms & regional cooperation
- Research and training **opportunities in many areas**
  - C4I & Cyber, C2SIM, Peace Simulation Network, comprehensive approach environments. Use International Transformation (ITX) Chairs
- Consider **regional knowledge** development resources (now European & Mid-East initiatives—add ASEAN (??))
  - Analytics & visualization component
  - Training modules and a vibrant community of interest
- **All could be tied together**



# QUESTIONS?

[linwells@gmail.com](mailto:linwells@gmail.com)

Skype: linwells

U.S. cell +1 202.436.6354