
A Framework to place Naval Warfare, Naval Systems, and Cyber Warfare in Context & What Annapolis is doing to Prepare

ICOF 2015 Meeting

Annapolis

(note: Framework published by SECNAV 3 May 2015)

<http://www.secnav.navy.mil/innovation/Pages/2015/4/MacroRevolutions.aspx>

7 May 2015

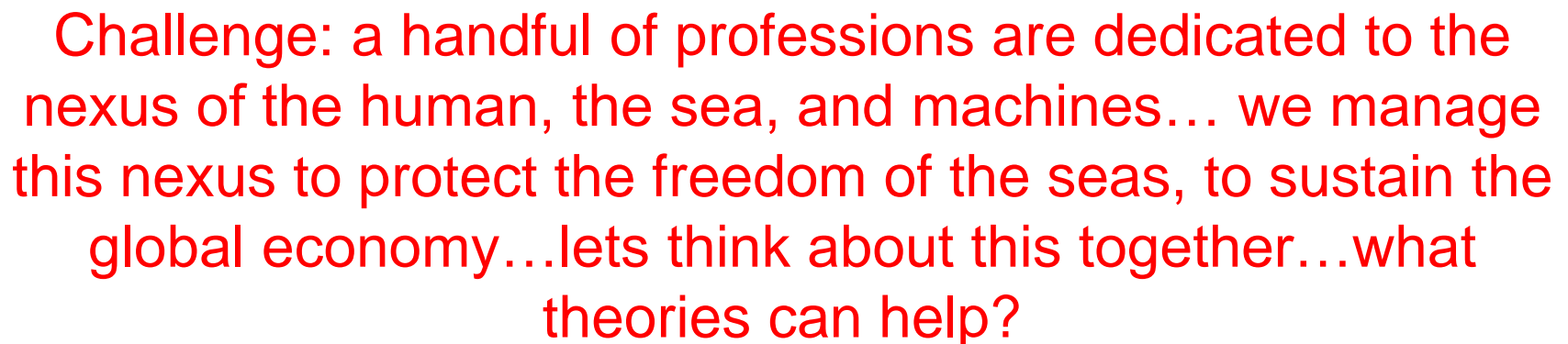
Mark Hagerott CAPT USN (ret) PhD

Deputy Director, USNA Cyber Center

hagerott@usna.edu

410.293.0937

□Note: The views and opinions of authors expressed herein do not necessarily state or reflect those of the U.S Navy or the United States Government





1. Life Cycle Theory of technological change
2. Cybernetic Theory of War/Activity: Sense-Think-Act
3. The New Change: Emergence of a “Third Realm” of War/”Third Realm” of Economic Activity, near simultaneous with system-wide “cyber vulnerability”

Gain Perspective: step back and look at the historical trajectory/trend of technology....

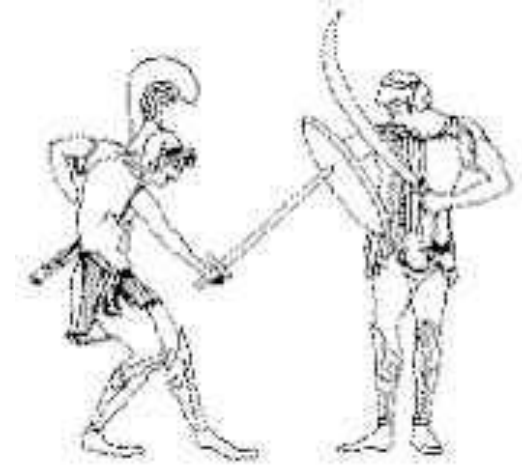
- ❑ “ ... because our teachers ...focus their attention only on the present or at the most on the very recent past, they find the present more and more difficult to explain. They are like oceanographers who refuse to look at the stars because they are too remote from the sea, and consequently are unable to discover the causes of the tides.”

Marc Bloch, French historian and veteran of WWI and WWII, tortured and killed by the Gestapo while fighting as part of the French Resistance

A Tool and Framework for Thinking...

At first...there existed one realm of warfare/activity: the Social-Human Realm

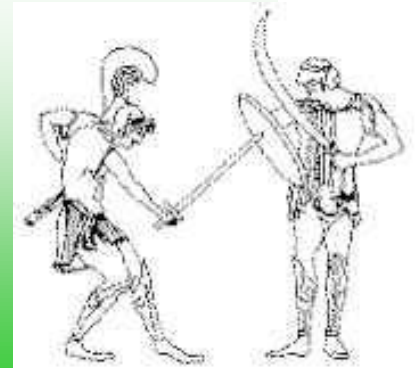
- ❑ Most of history and pre-history, the social-human factor was decisive action in war:
 - Human wit, will, strength, and ability to persuade....
 - Tools magnified or leveraged human strength, or protected the human body.
 - Humans dominated the Sense-Think-Act sequence



One Realm of Warfare....‘Social-Human’ factors dominate Sensing-Thinking-Acting

Social-
Human
Factors
Dominate
S-T-A

Social- Human
Realm



Enter Accelerating Technological Innovation,
Increasing Complexity, and the more tools to
better Sense-Think-Act (S-T-A)

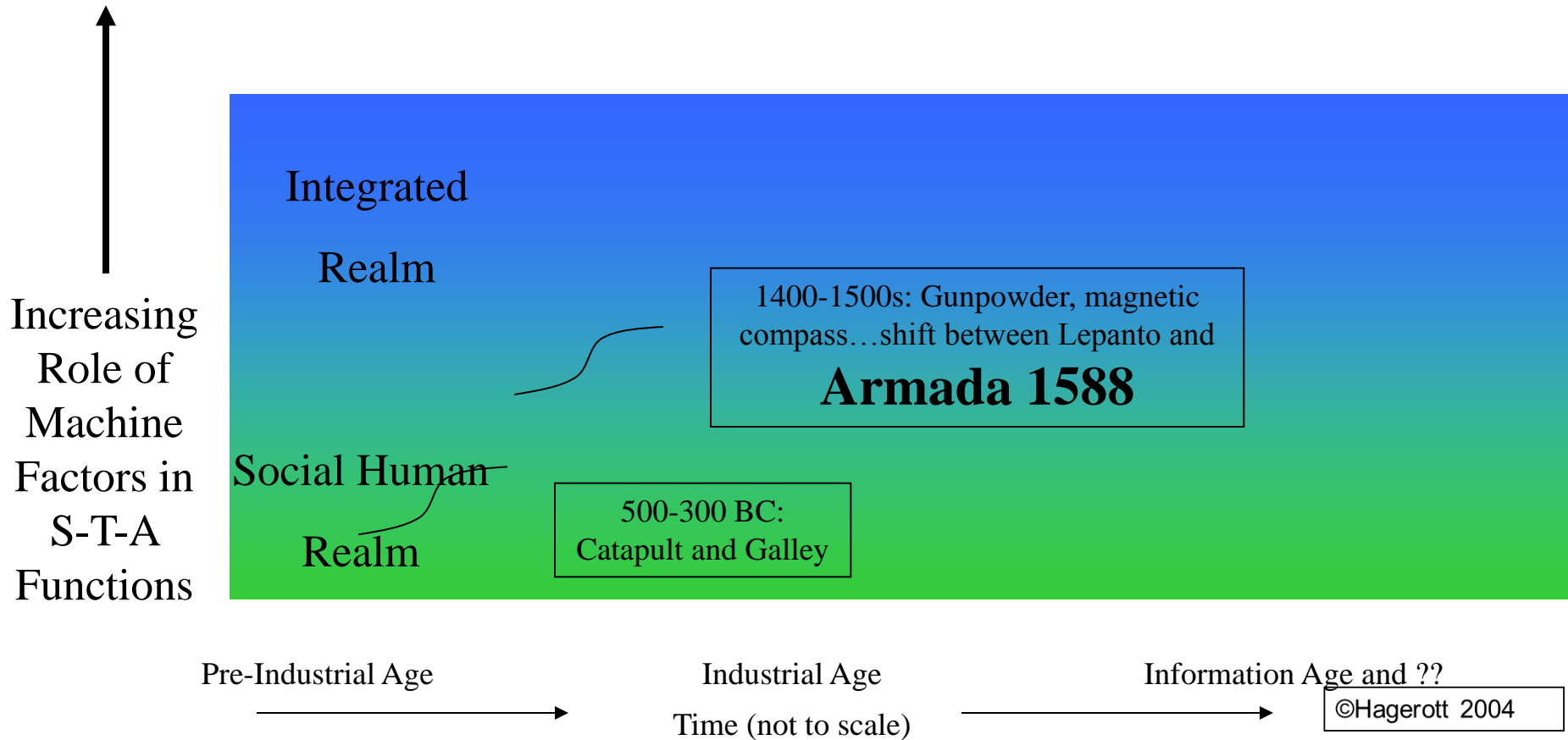
Integrated Realm emerges...Machines and specialists replace human mass...first at sea



Social-Human Realm: 1571 Battle of Lepanto dominated by mass infantry battles fought on/across fleets of galleys....

To Integrated Realm: 1588 Battle of Armada the English embark **ZERO INFANTRY** and fight an artillery duel at sea on 'ships of the line'

Waves of Innovation increases Human-Machine S/T/A integration in war...evolving the 2nd Realm



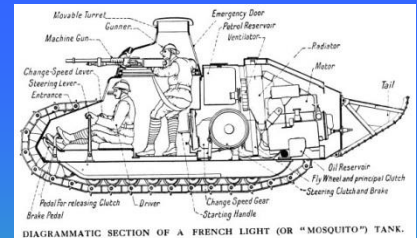
Now...two Realms of warfare co-exist...



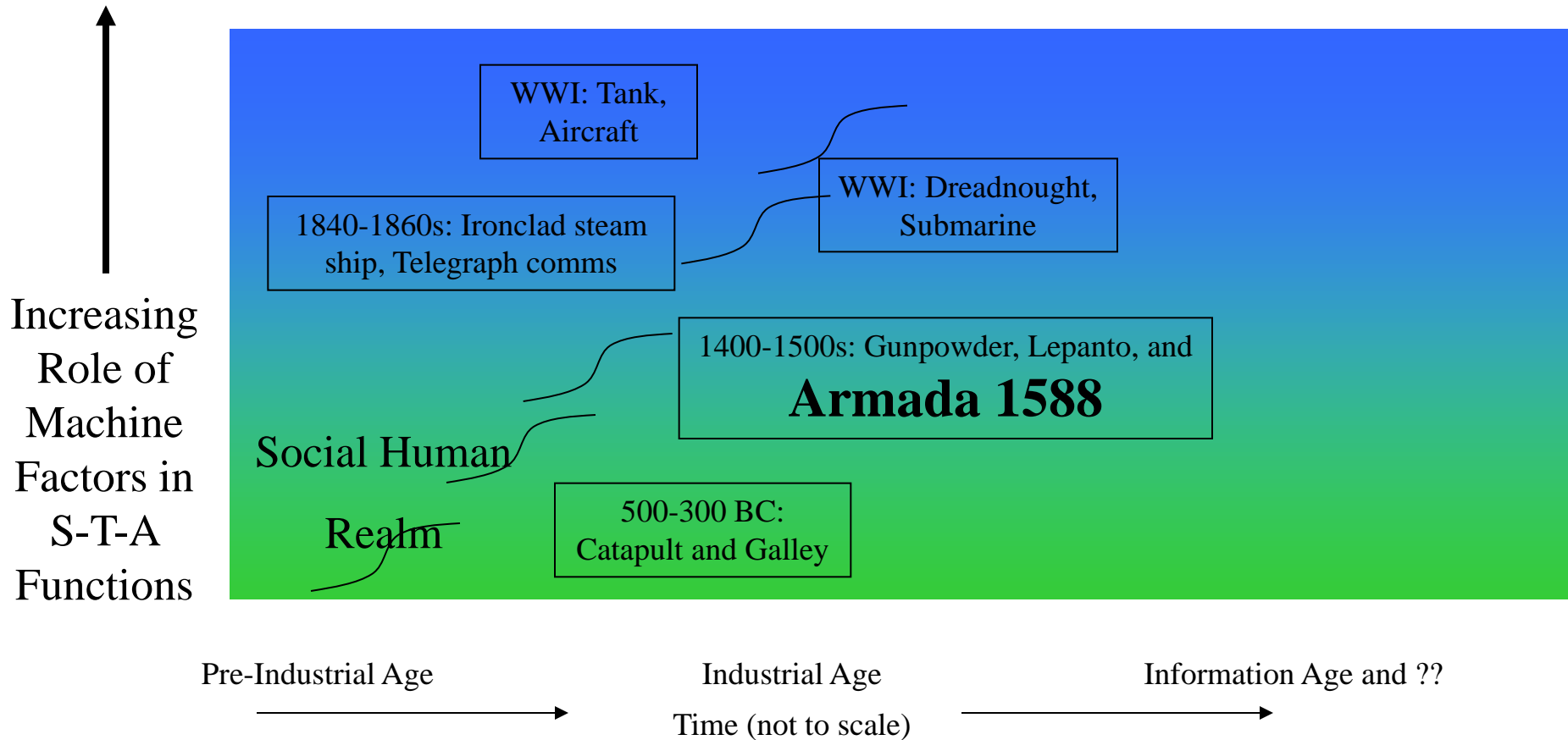
Increasing
Role of
Machine
Factors in
S-T-A
Functions

Integrated
Realm

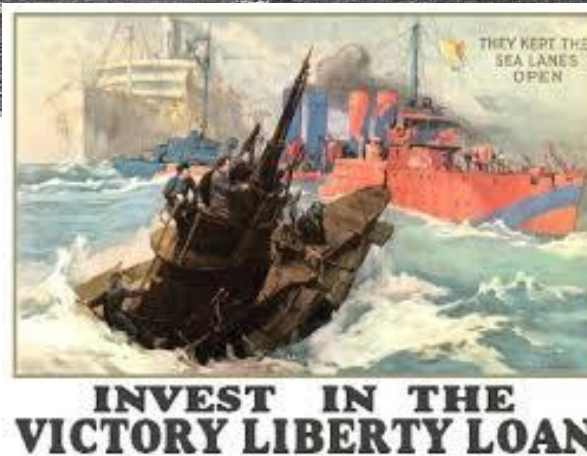
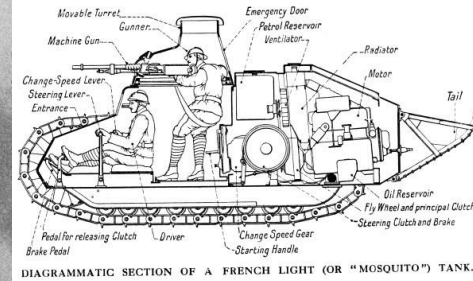
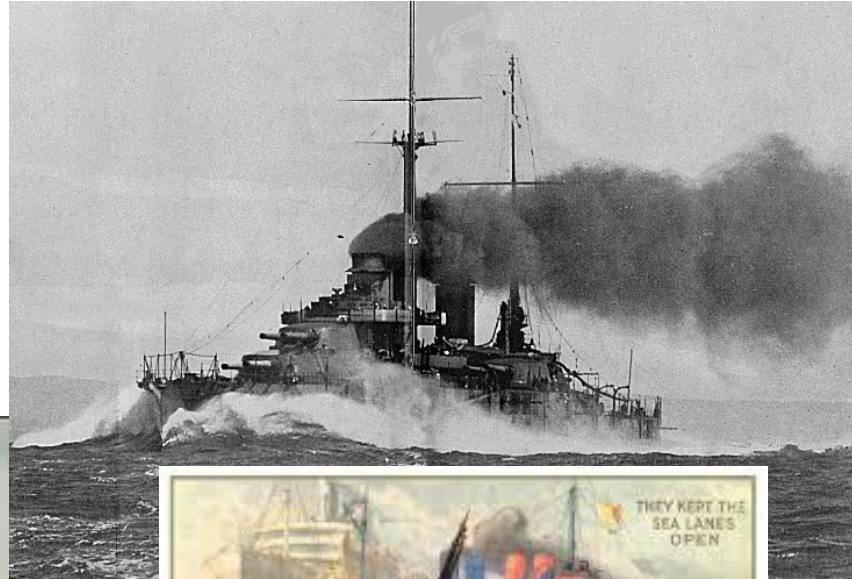
Social- Human
Realm



Waves of Innovation... more Complex Machines Assume Increasing Role in the Sense-Think-Act Function



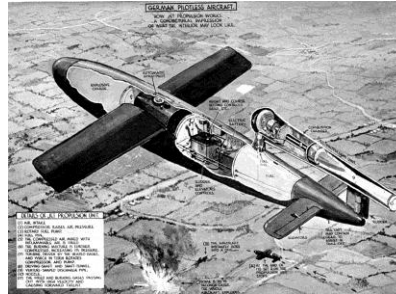
Increasing integration of the Human and Machine ... Integrated Realm



“Artillery men with their cold blooded mathematics seemed subversive of all that made a soldiers life heroic, admirable, worthy.” William McNeill, Pursuit of Power)

20th century Scientific Engineering creating the third and final realm of warfare: “Machine Realm”

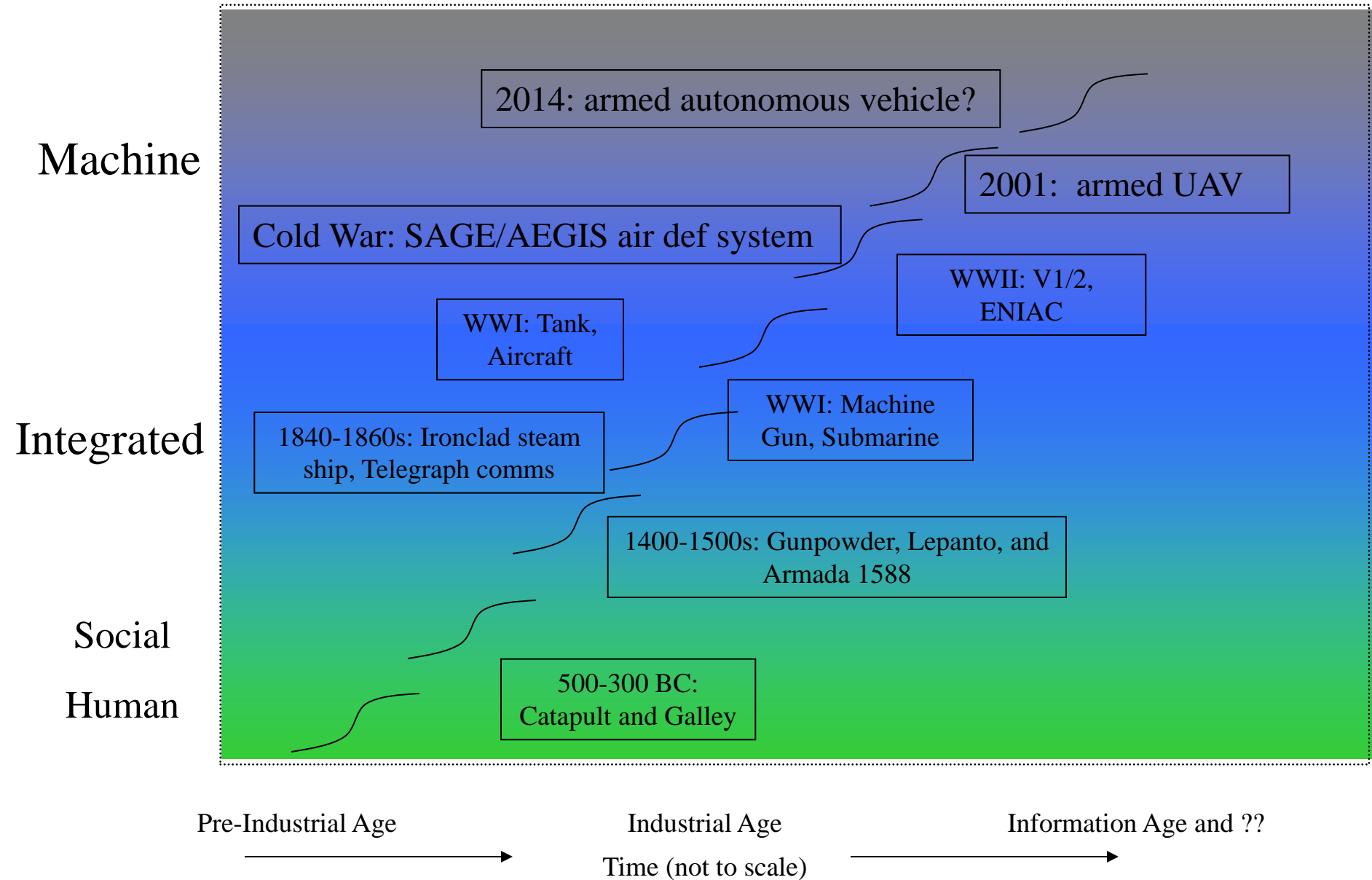
- ❑ With the increased complexity came an increased machine capacity for sensing, thinking, acting at higher speeds...the ‘MACHINE Realm’ emerges



“...modern warfare is more a matter of machines than of men.” Thomas Edison, 1913

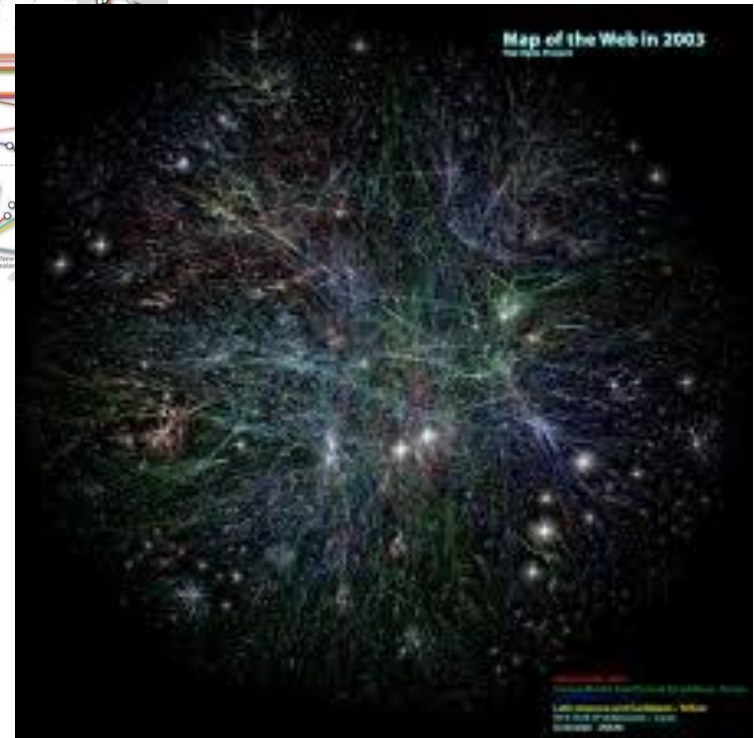
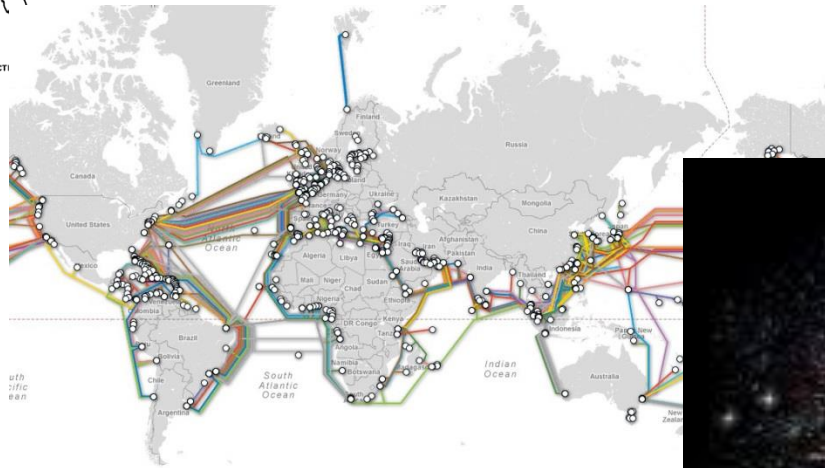
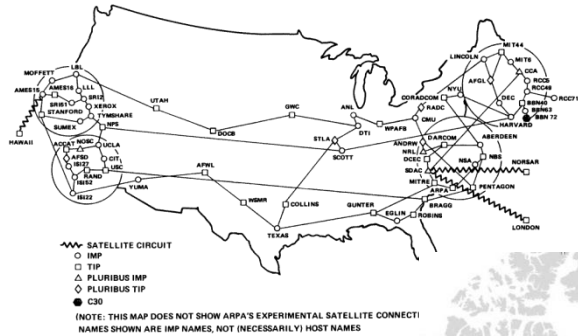
Micro-waves of Innovation push into the Third Realm of AI, Autonomous Machine War...Standby for Disruption!!

Unclassified



Internet/Wireless Growth is building Attack Vectors...across all Realms of War

ARPANET GEOGRAPHIC MAP, OCTOBER 1980



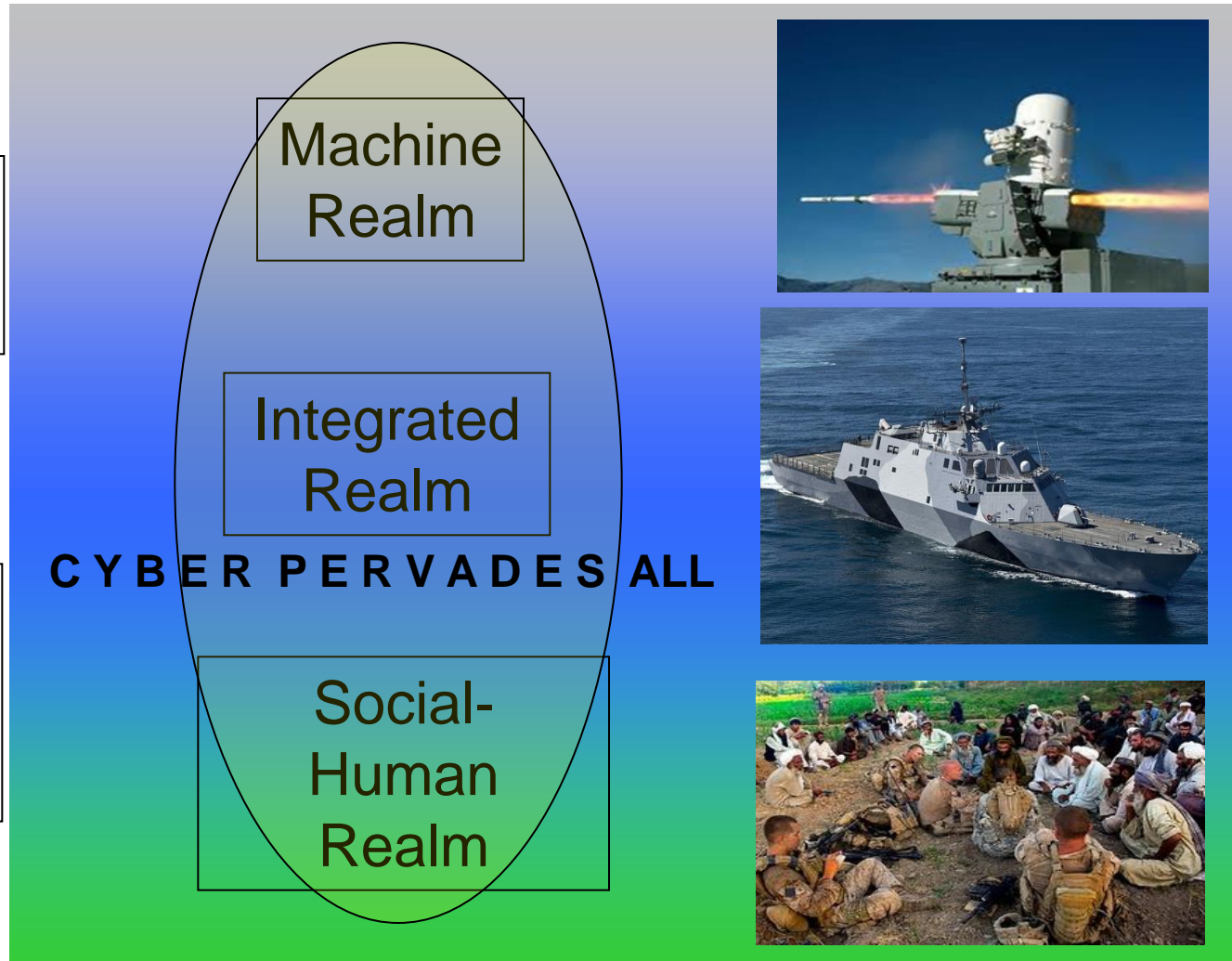
A New Reality...Three Realms of War



**Machine
Factors More
Decisive**

Role of Machine
Factors in S-T-A
Functions

**Social-Human
Factors more
decisive**



Cyber Pervades all Three Realms

Cyber Insecurity will slow the Robotic Revolution or Accelerate the move to autonomy?



Automated Systems... more discriminating, thus more ethical? Maybe... But certainly not if cyber systems are compromised and corrupted....(see Ron Arkin, Michael Smith, et al on drone ethics). See Danzig recent paper.

Unclassified Apply the Framework to Current Events/Future Possibilities



**Super A.I.
breakthru**



**Machine
Factors More
Decisive**

Role of Machine
Factors in S-T-A
Functions

**Social-Human
Factors more
decisive**



ISIS



Machine
Realm

Integrated
Realm

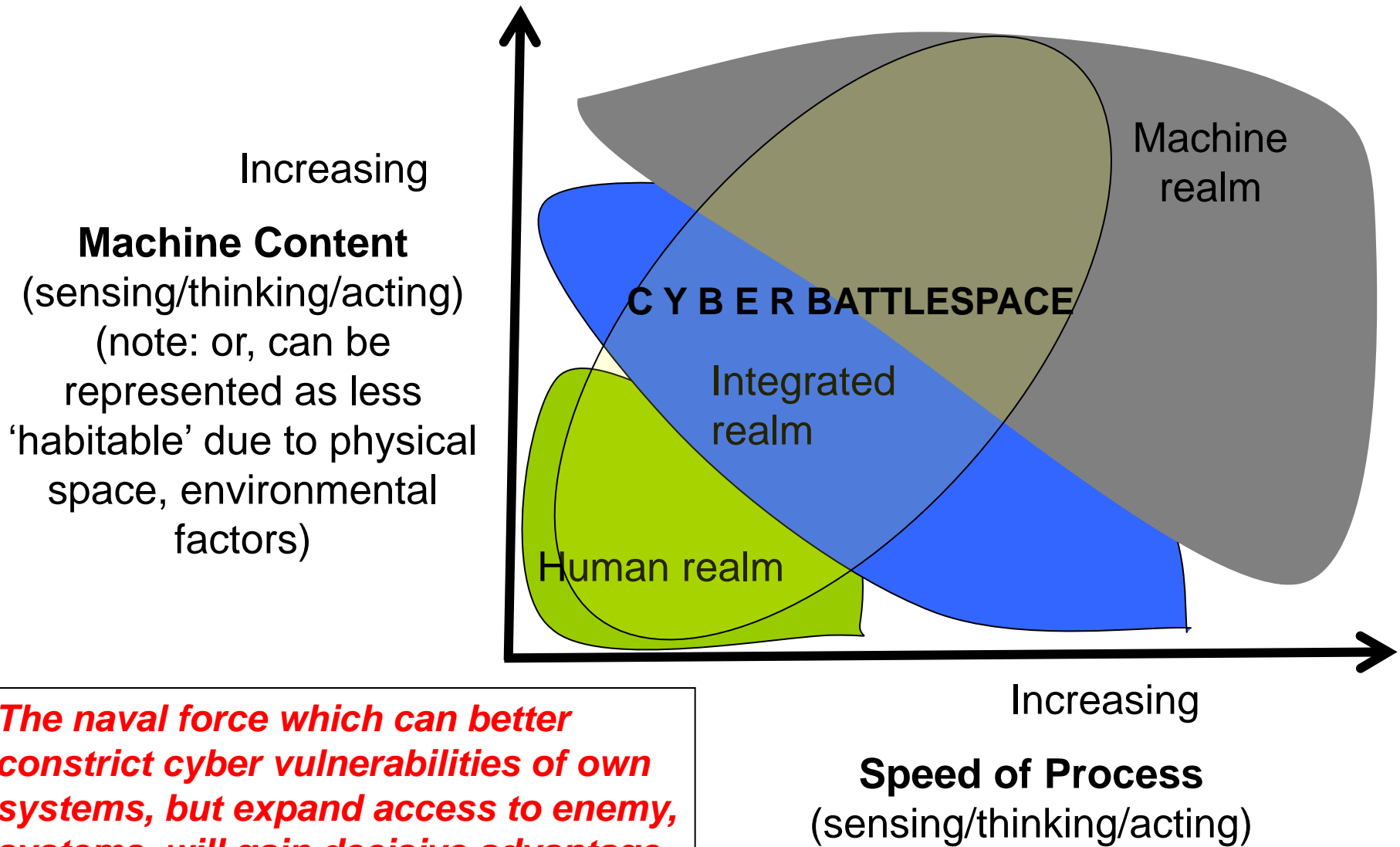
**CYBER PERVADES ALL
Realms... but with limits...**

Social-
Human
Realm



Range of Cyber tools can be limited by tech... or lack of tech

Cyber technologies, both defensive and offensive, will battle to penetrate or shield the three realms of activity



The naval force which can better constrict cyber vulnerabilities of own systems, but expand access to enemy systems, will gain decisive advantage.

Unclassified Apply the Framework to Current Events/Future Possibilities



**Super A.I.
breakthru**



**Machine
Factors More
Decisive**

Role of Machine
Factors in S-T-A
Functions

**Social-Human
Factors more
decisive**



Insider Threat



Machine
Realm

Integrated
Realm

**CYBER PERVADES ALL
Realms... but with limits...**

Social-
Human
Realm



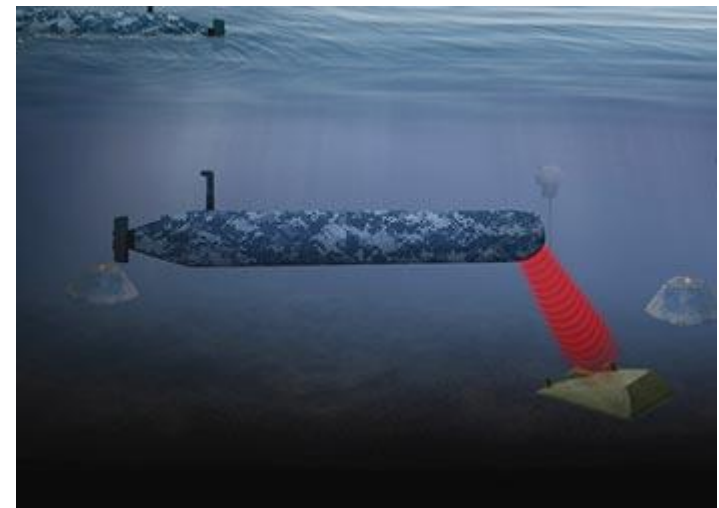
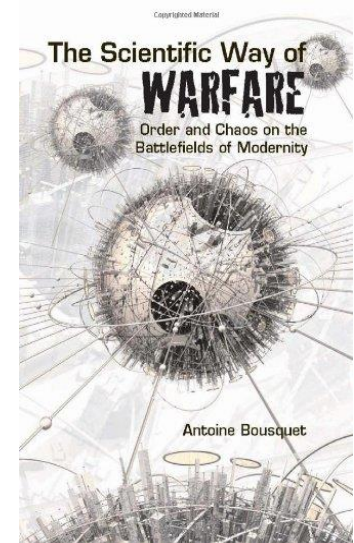
Range of Cyber tools can be limited by tech... or lack of tech

Disrupting How we Sense-Think-Act...Communicate, Command, and Control



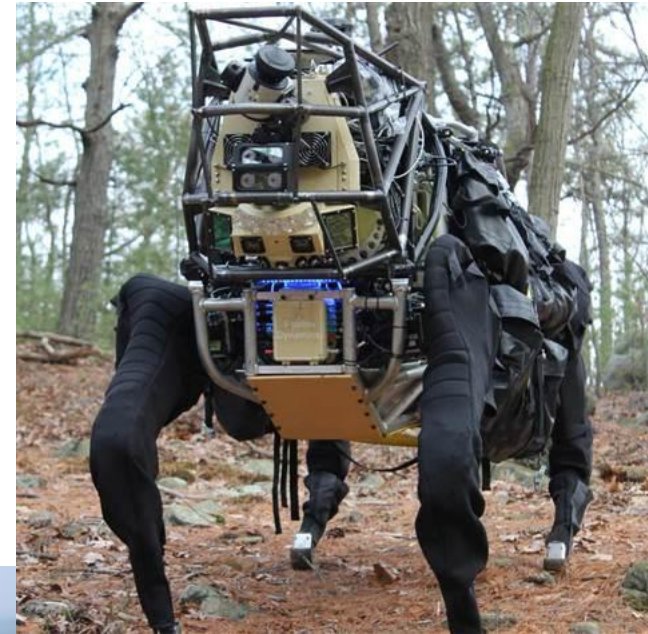
Disrupting How We Provide Security/Defense

Unclassified



Unclassified

Disrupting Budgets/Programs...



When Paradigms Change...what type of officer is needed?

- ❑ Strike a balance between specialists and integrators.



Naval Aviators #1 Lieut. T. Gordon "Spuds" Ellyson, left, and #3 Lieut. John Towers

Photo # 80-G-35725 Lt. R.H. O'Kane & LCdr. D.W. Morton on bridge of USS Wahoo, circa Feb. 1943



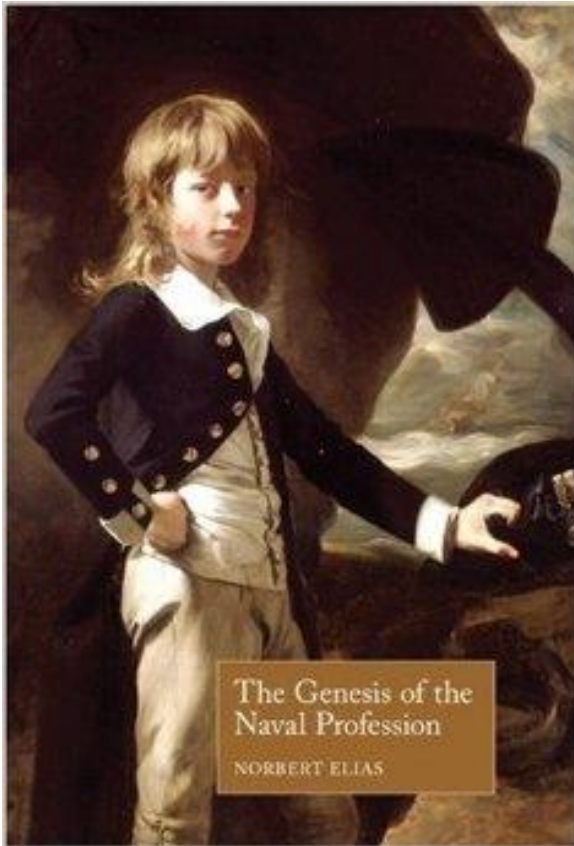
Photo # NH 50033 Naval Cadet Ernest J. King, ca. 1901



Submarine skippers shown above look young... where are the "old guys"?



Cyber... disrupting Education



Cyber... disrupting Career Paths, Creating New Organizations

Unclassified



Unclassified

Summary: Confluence of Two Events will Challenge the Maritime Professions!

Unclassified

- ❑ Two near simultaneous challenges:
 - ❑ 1. Emergence of a Third Realm: Autonomous Machine War (while the other two remain intact)
 - ❑ 2. Electronic Netting of the World of Humans and Machines...the 'cyber' phenomenon

The USNA Cyber Program

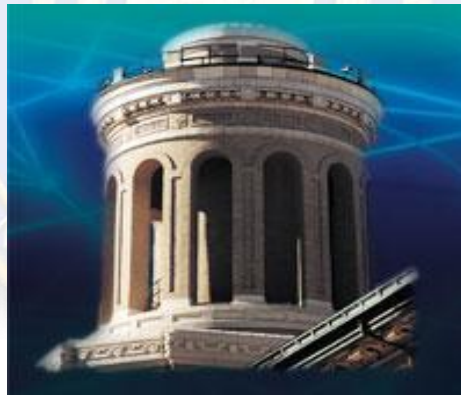
Turning Midshipmen into Cyber Warriors



CAPT Paul Tortora, USN
Director, Center for Cyber
Security Studies

CCSS Mission

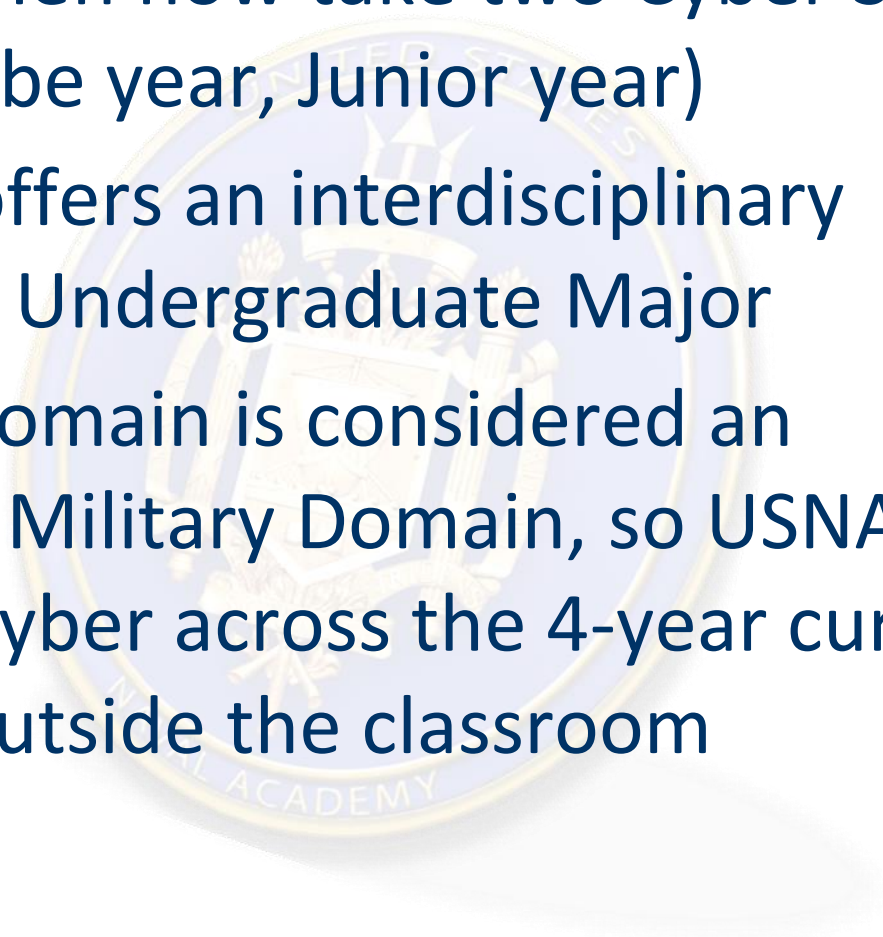
To enhance the **education of midshipmen** in all areas of cyber warfare, to facilitate the **sharing of expertise and perspective in cyber warfare** from across the Yard, and to enhance **inter-disciplinary research** in cyber warfare at USNA.



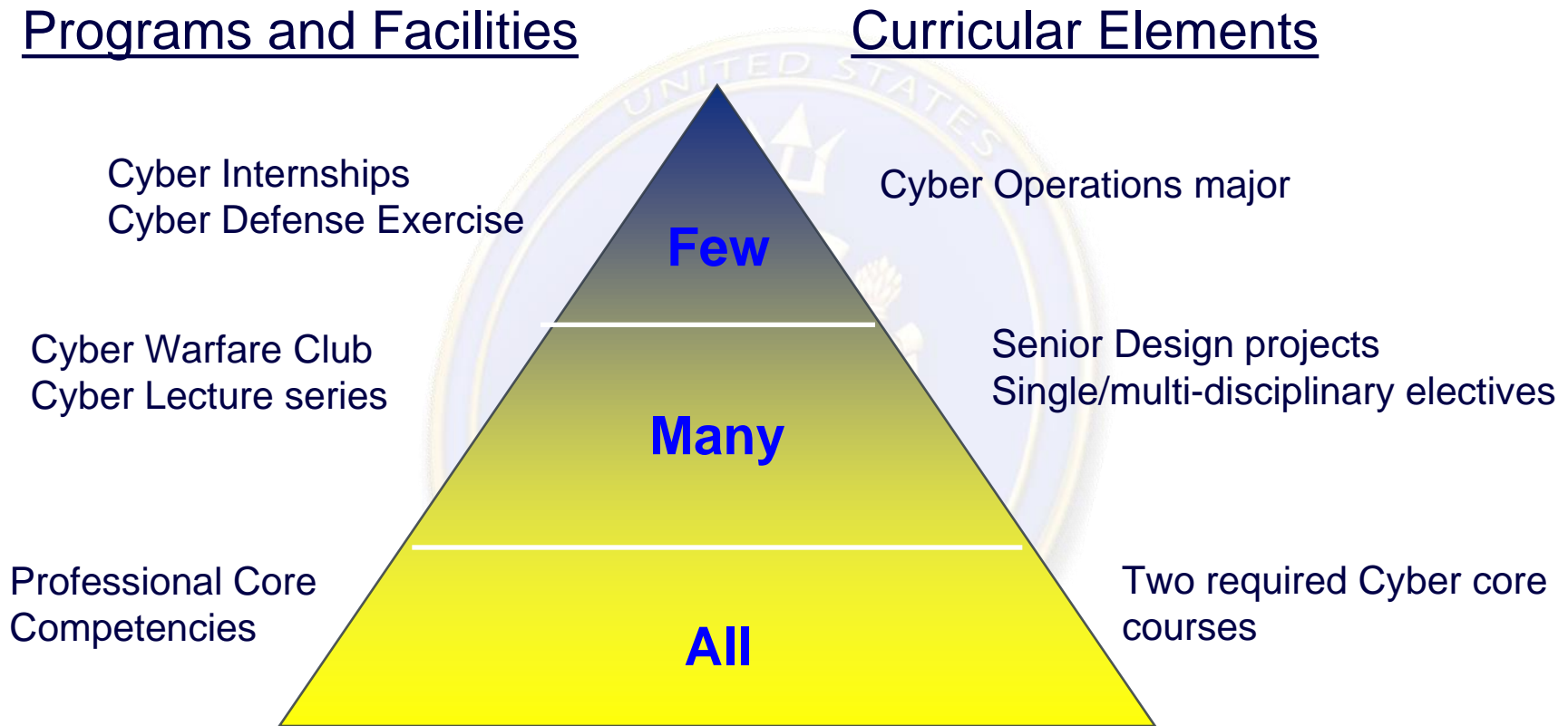
Transforming the Navy 1,100 Midshipmen at a time



Bottom Line Up Front

- All Midshipmen now take two Cyber Security Courses (Plebe year, Junior year)
 - USNA now offers an interdisciplinary “Cyber Operations” Undergraduate Major
 - The Cyber Domain is considered an Operational Military Domain, so USNA is expanding Cyber across the 4-year curriculum, inside and outside the classroom
- 

Overview of Cyber Education at USNA



Goal: Prepare Graduates to Lead in an Evolving Cyber Domain



Plebe Cyber: Structure & Content

Cyber Battlefield: Defining the Digital World

Digital Data: Bits & Bytes (0's & 1's)	Basics of Computer Components	System Overviews: Windows, Linux	Basics of Coding & Scripting	Basic Web & HTML	Client & Server Side Scripting	Web Injection Attacks	Networking Basics, Ports Protocols	Wired & Wireless Network
--	-------------------------------	----------------------------------	------------------------------	------------------	--------------------------------	-----------------------	------------------------------------	--------------------------



Security Tools: Information Assurance

Symmetric, Asymmetric Encryption	Hashing & Passwords	Cryptography/ Digital Cryptography	Digital Certificates Lab	Network, Port security, Firewalls	Steganography, Hidden files, File Security	Network Risk assessment
----------------------------------	---------------------	------------------------------------	--------------------------	-----------------------------------	--	-------------------------



Cyber Operations: Attack & Defense

Digital Forensics, Basic Forensics Lab	Malware, Attack Vectors Case Studies	Phases of a Cyber Attack & Cyber Reconnaissance	Cyber Attack Discussion, Cyber Attack Lab	Cyber Defense, Cyber Defense Lab, All-out Attack Lab
--	--------------------------------------	---	---	--



Cyber 2 – Junior Year

Operational Cyber Security

Operating Systems,
Assembly Language
Basics

Data Management /
Memory
Management

Privilege
Management

Buffer Overflow &
Prevention

Network Protocol
Hierarchies and
Reference Models

Internet /
Network
Layers

Transport Layer
Security



Electro-Magnetic/EW Spectrum

Principles of the
RF Spectrum

Signals, Gain,
and dB

Bandwidth
Sharing/
Multiplexing

Digital Modulation
Schemes /
Information
Theory


Antennae and
RF Propagation

Eavesdropping,
Jamming,
Spoofing

Spread
Spectrum

Frequency
Hopping

***Enhancing Midshipmen Understanding of Cyber Operations
and Use of the Electro-Magnetic Spectrum***

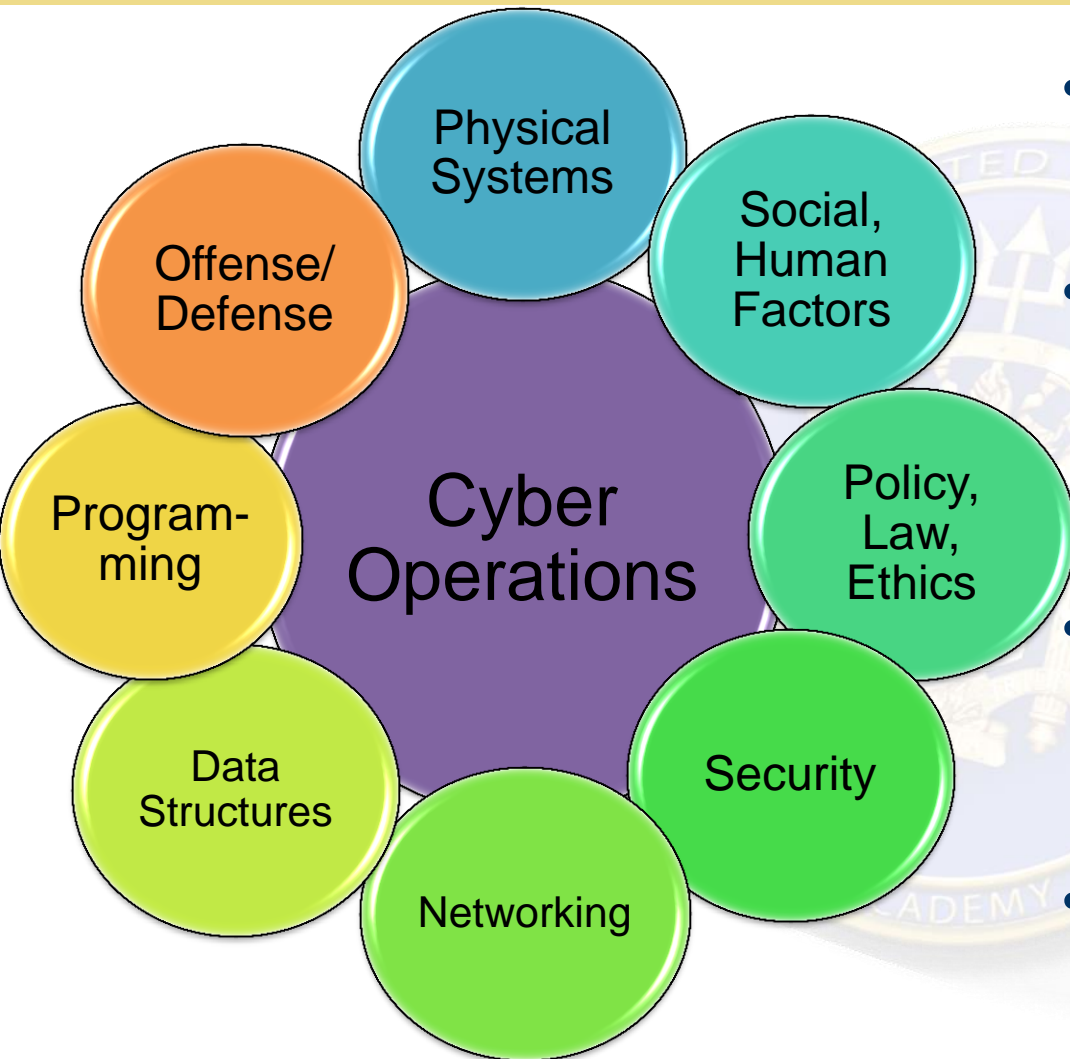


New Cyber Operations Academic Major

- Initiated last Academic Year (one of 25 Academic Majors)
 - 28 MIDN from Class of 2016 in the major
 - 59 from Class 2017
- Interdisciplinary approach in its inception and execution
 - Developed with inputs from all departments
 - 50 credits for major, 142 total credit loading
 - Professors and Military faculty from across academic departments
- Cyber context drives each course in the major
 - New courses distinct from existing ones
- SCY is a technical (STEM) major, but maintains 3-5 non-technical courses to keep an appropriate balance
- Seeking ABET Accreditation with similar programs nationwide

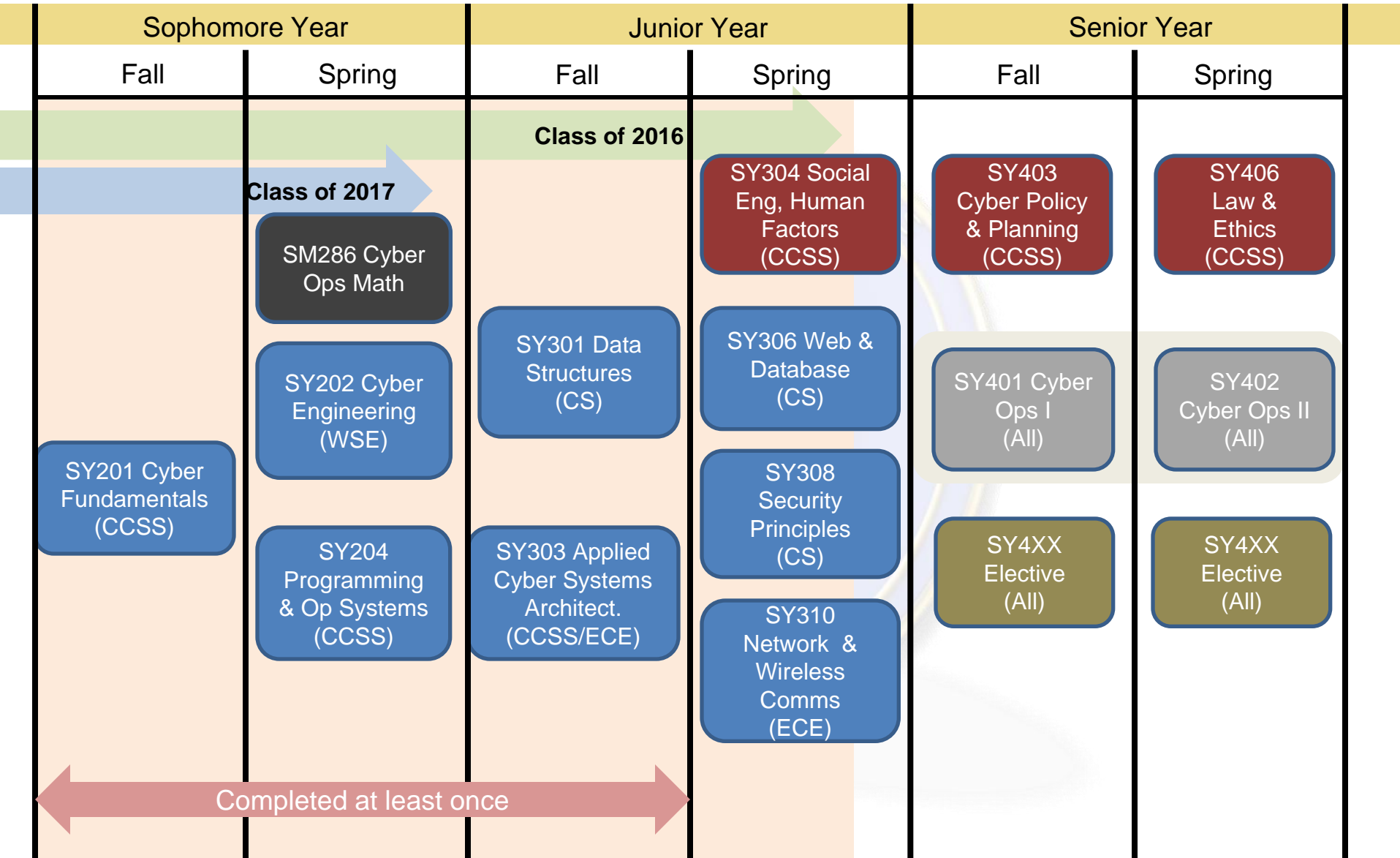


New Cyber Operations Major



- Initiated last Academic Year
 - 28 MIDN from Class of 2016, 50 from Class 2017, 32 from 2018
- Interdisciplinary approach in its inception and execution
 - 50 credits for major, 142 total credits
 - Professors & Military faculty from across academic departments
- Cyber context drives each course
 - Courses distinct from existing ones
 - Technical (STEM) major, but has non-technical required courses
- Seeking ABET Accreditation with similar programs nationwide

Cyber Operations Major





Cyber Operations Major Courses & Content

Technical Courses

- Cyber Fundamentals
- Cyber Systems Engineering
- Programming
- Web / Database For Cyber
- Data Structures
- Architecture (H/W Plus Assembly Language)
- Networking & Wireless Comms
- Systems Programming / OS Fundamentals
- Security Fundamental Principles
- Cyber Offense / Cyber Defense

Non-Technical Courses:

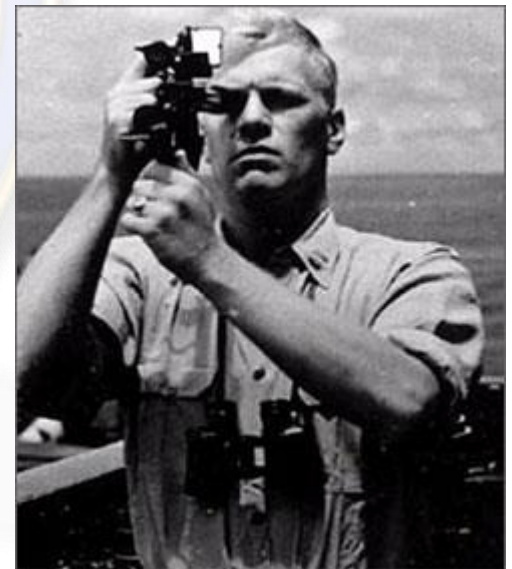
- Cyber Planning & Policy
- Cyber Law/Ethics
- Social Engineering (Cyber Psychology)

Electives (2 from below):

- History of Technology & Cyber-warfare,
- Applied Cryptography,
- Cyber Defense Strategies
- SCADA
- Mobile Programming
- Forensics
- Other: NSA, DOD, Navy and Civilian Cyber-related Internships, projects being expanded

If the Machines Stalemate...Do We Have Skill...Do we have Understanding...Grit

- If the automated cyber security systems become matched? Does machine stalemate result?
- If so, does advantage shift to the HUMAN workforce...
- Who can 'manually' debug/restore the system faster than the other guy?
- Who can navigate with degraded electronics... without GPS?





CCSS Staff & Faculty

- A desired blend of
 - Operational Fleet and Interagency experience
 - Technical experts (CS, EE, WSE)
 - Experts on attack and defense techniques
 - Policy / law experts
 - World-class thought leaders who are helping to create the nation's policy and law
 - Currently heavily reliant on other USNA departments, but we are seeking to hire full-time cyber faculty
- Goal: LEAD the nation in undergraduate cyber operations education and beyond

The Many: CCSS Lecture Series



- **ADM Dennis Blair**
- **ADM Mike Rogers**
- **Kevin Mandia**
- **Dr. Martin Libicki**
- **GEN James Cartwright**
- **GEN Mike Hayden**
- **GEN Keith Alexander**
- **Mr. David Gompert**
- **Jane Holl Lute, DHS**
- **Mark Bowden**
- **Richard Clarke**
- **Kevin Mitnick**



Proposed Cyber Building



- FY15 Budget Item: \$120M for construction, target completion 2019
- Will co-locate similarly focused academic majors:
- Cyber Operations, Computer Science, Information Technology, Computer Engineering, Systems Engineering and Electrical Engineering
- Will have several SCIF classrooms and secure lecture space

Backups





Cyber 1 – Plebe Year

- Mandatory for all USNA students starting with Class of 2015, our current seniors who will be the “*bow-wave*” of enhanced Cyber awareness to the Fleet
- Course focuses on cyber operations
 - Context motivated by current events
 - Technical emphasis; non-technical related to *context*
 - Fundamentals of risks and threats
 - Hands-on experiences
 - Tie-in topics to Fleet operations when possible



Cyber 2 – Junior Year

- Started last year (Class of 2015)
 - Technical focus; non-technical context
 - Emphasize networks and electrical/electronics applications
 - Deeper awareness and understanding of the cyber realm
- Project Based Learning focus
 - Initially based on required EE course, modified to provide Cyber/IW/EW context
 - Requires laptops and lab equipment
- Topics that directly relate to Communications and use of the Electro-Magnetic Spectrum in the Fleet

Backups for Framework Section
