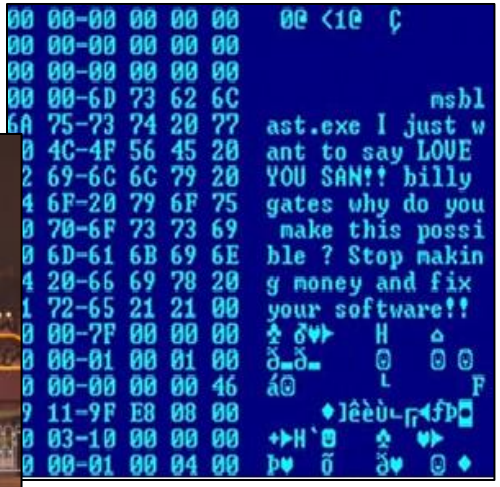
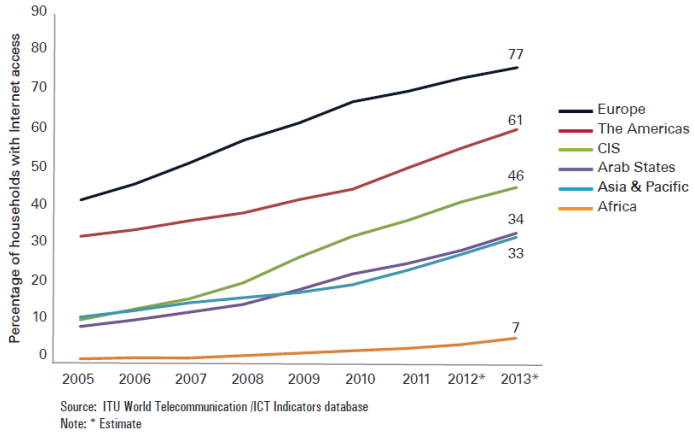
Information

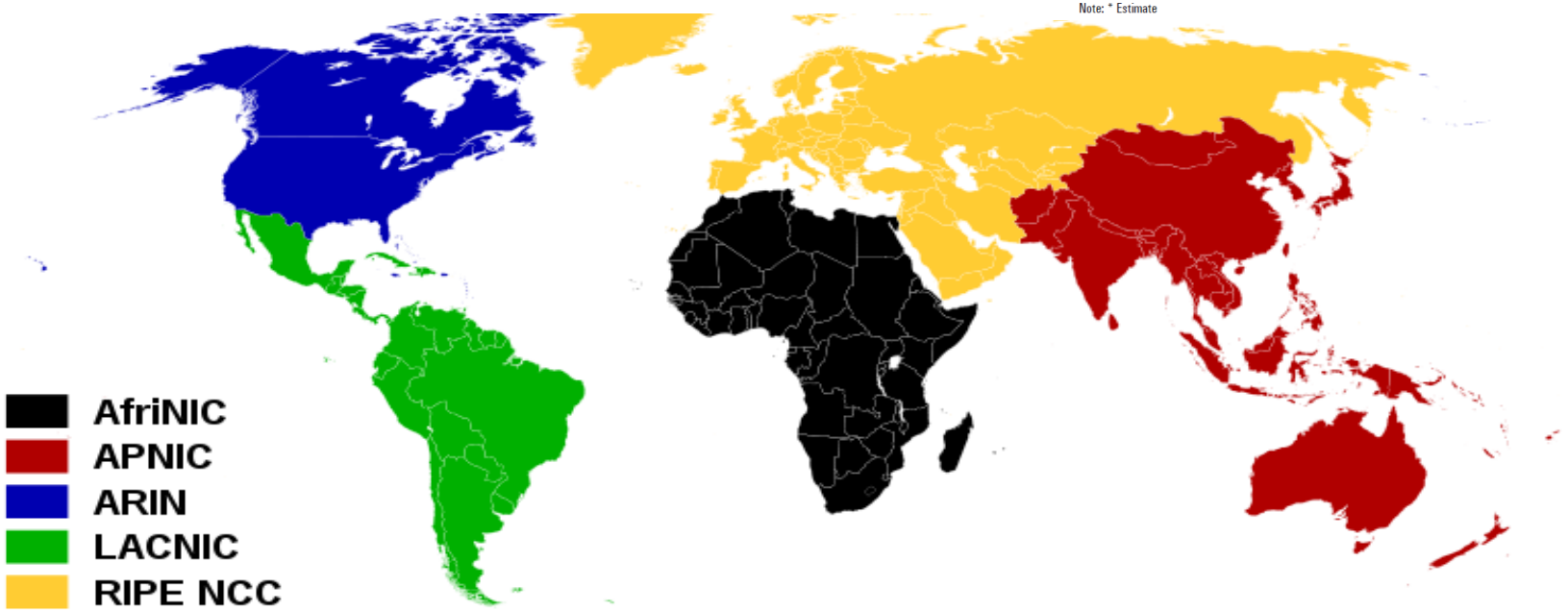


The Information Environment is Global

- ***2.7 billion people – almost 40% of the world's population – are online.***
- ***There are 6.8 billion total mobile subscriptions almost as many as people in the world, with more than half in the Asia-Pacific region (3.5 billion).***
- ***75% of the global population owns a mobile device.***



Source: ITU World Telecommunication /ICT Indicators database
Note: * Estimate



Regional Internet Registries World Map

IE Operational Realities

- ***Information Communications Technology (ICT) Accessible to anyone***
- ***No one owns the internet in its entirety resulting in sovereignty problem***
- ***Gives military capability to groups not traditionally associated with those capabilities***
- ***ICT is a double edged sword needed by the Threat and Friendly forces***
- ***INFOWAR offers opportunities for low risk high pay off operations***
- ***INFOWAR is misunderstood by many commanders because of unknown technology***
- ***Difficult to assess damage***

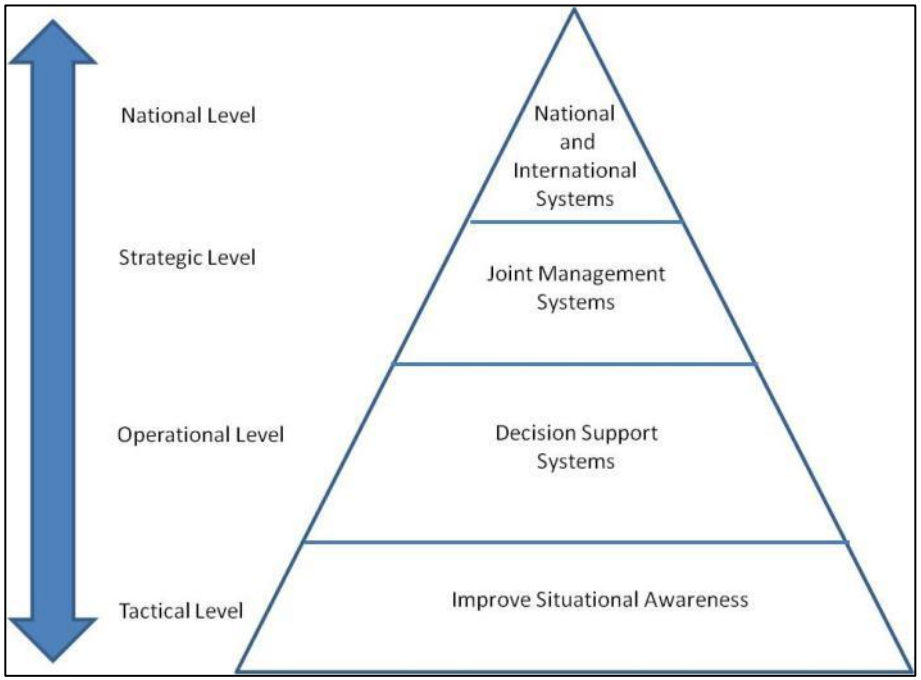
Elements of Information Systems

•Computer hardware: A collection of physical elements that comprise a computer system or network.

•Computer software: A collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it.

•Data analysis: A process of inspecting, cleaning, transforming, and modeling data with the goal of highlighting useful information, suggesting conclusions, and supporting decision making.

•Purpose: Provides information which is needed to manage organizations efficiently and effectively



Leveraging Information in Training

- Bad Information- Deception and disinformation causes a lack of trust in the decision making process.
- Too Much Information- Competing priorities and real time reporting stresses C2 systems.
- Not Quite Enough Information- Key information requirements lack the necessary detail to make a decision.
- Perfect Information- Unprecedented situational awareness.

Information Warfare

Information Warfare

"Specifically planned and integrated actions taken to achieve an information advantage at critical points and times. The goal is to influence an enemy's decision making through his collected and available information, information systems, and information-based processes, while retaining the ability to employ friendly information, information-based processes, and systems." TC7-100.2 OPFOR Tactics

Concepts of Information Warfare

- Information Infrastructure- Considered high value targets or areas of interest

- Blurring of Boundaries- Area of influence includes the info space as well as the physical area

- Expanded Role of Perception Management- Every operation has a perception management element

- Vulnerability of Technology- Commercial technology and over reliance on technical solutions puts military operations at risk

- Neutralizing Superiority- Simple countermeasures can degrade technical overmatch

ELEMENTS OF INFOWAR

- Electronic Warfare (EW).
- Deception.
- Physical destruction.
- Protection and security measures.
- Perception management.
- Computer Warfare/Information Attack (CW/IA).

Electronic Warfare

Objective:

Exploit, disrupt, deny, and degrade the enemy's use of the electromagnetic spectrum

Target:

Command and control assets and information networks and systems

“Networked and dispersed jammers”

- Instead of Soviet-style blizzard jamming from large, semi-fixed jammers, Threat will field small distributive jammers
- These jammers will be both fixed and mobile (ground vehicle/UAV)
- These jammers can be controlled though civilian cell phone networks, or controlled by local forces
- Along with known military frequencies, threat will target civilian (NGO, US civilian) and host nation radios/cell phones

Impact to the Warfighter:
- Loss of GPS/Comm/Data links-Blue Force Tracker (BFT), Personal/Unit Communication could be degraded
- Muddles Common Operating Picture (COP)
- Intel feed to/from TOC could be reduced
- Jammers can be used as bait for ambushes, with the resulting ambush videoed and used for perception management operations
- Units could potentially be forced onto less secure communications

Pocket RF Jammer

"GPS SPOOFING"

- Threat will attempt manipulate GPS or like systems by inputting incorrect data, creating positional errors
- GPS is hardened against spoofing, but not invulnerable to this type of attack
- GPS is considered by both friend and foe to be the critical enabling technology advantage of the US
- Navigation, Blue Force Tracking, Survey, Gun/Mortar Alignment, Targeting, Sensors, Weapon Guidance, Timing, Logistics Tracking and Aviation operations will all be effected
- Supporting arms and secure comms depends upon accurate GPS

Impact to the Warfighter:

- Remediating Attack effects to determine positional error would be time-consuming
- Incorrect location can cause fratricide or other accidents
- Command and Control confusion
- Friendly Force speed advantages in targeting, movement and coordination could be reduced or eliminated by positional confusion

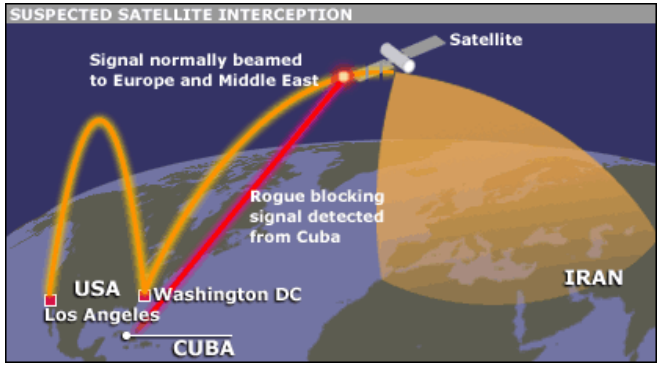
“SAT jamming”

- Satellites, especially UHF, are vulnerable to uplink jamming
- Loss of SATCOM connectivity by even low power jammers would represent a significant loss of connectivity between BCT elements and the BCT to other echelons
- SATCOM is an essential element to the BCT CO for both Corps and higher connectivity and connectivity to far-flung assets
- Threat in the defense is far less likely to depend on SATCOM (having access to civilian infrastructure) thus can attack in barrage jamming mode
- Example: FLTSATCOM satellites were rendered inoperative by Brazilian CB enthusiasts

Homemade Brazilian SAT uplink used to pirate FLTSATCOM transponders

Impact to the Warfighter:

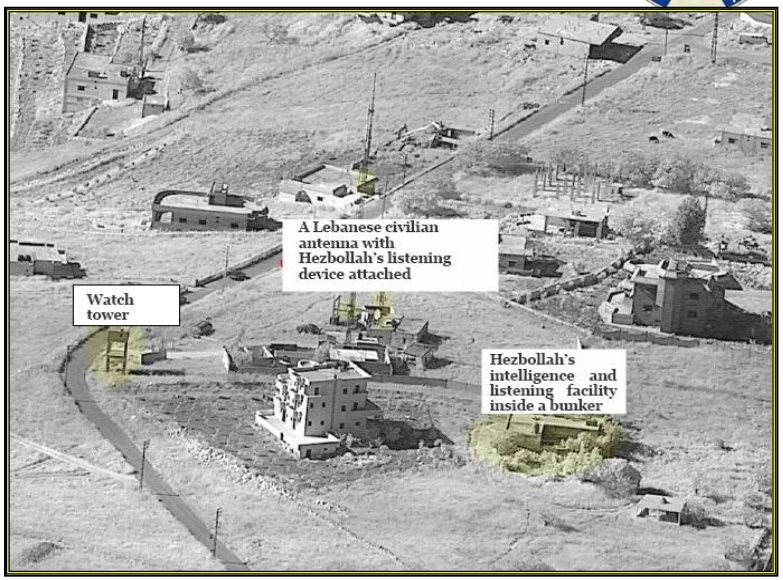
- Loss of SATCOM – no comms to higher HQ
- Assets like FLTSATCOM - used by a variety of US military and government users – are lost or degraded
- Units in mountainous terrain are particularly dependent on SATCOM
- Comms can be degraded or denied to some units



BBC diagram of probable Cuban Jamming of US source Iranian dissident TV; UHF jamming works similarly

“Monitoring Capabilities”

- Station receives Signals from many sources including , cellular communications and long range telephones
- Analysts located on site to perform COMINT and establish electronic order of battle
- Exploit civilian infrastructure and open source directories
- Mask communications by overwhelming the circuit and stressing monitoring capabilities



Impact to the Warfighter:

- Compelled to attack civilian infrastructure to defeat capability
- Unable to distinguish between threat and civilian targets
- Reduces freedom of action within the cyber electromagnetic spectrum
- Compromises OPSEC efforts

Deception

Objective:

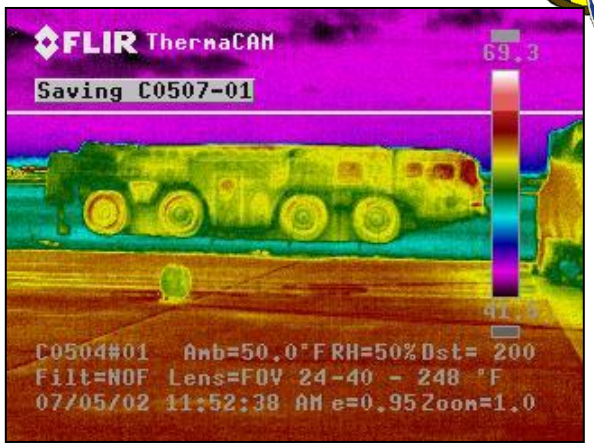
- Mislead enemy decision makers (military, political, diplomatic)
- Deceive populations to support OPFOR actions

Target:

- Range from tactical commanders to key decision makers for pol/mil/eco elite
- General population (internal and global) and media sources

"Smart Decoys"

- Smart decoys are distributed, controlled decoys designed to present a high fidelity (heat, electromagnetic, electro-optical and visual) simulation of a real vehicle
- Computerized controls will turn on decoy signatures to present a much more valid signature than previous generation "rubber duck" decoys
- Decoys will be emplaced in close proximity to prohibited targets (mosques/schools/hospitals) and civilian populations; if engaged, resulting civilian damage will be exploited in follow-on threat perception management operations



Scud launcher decoy with realistic thermal effects

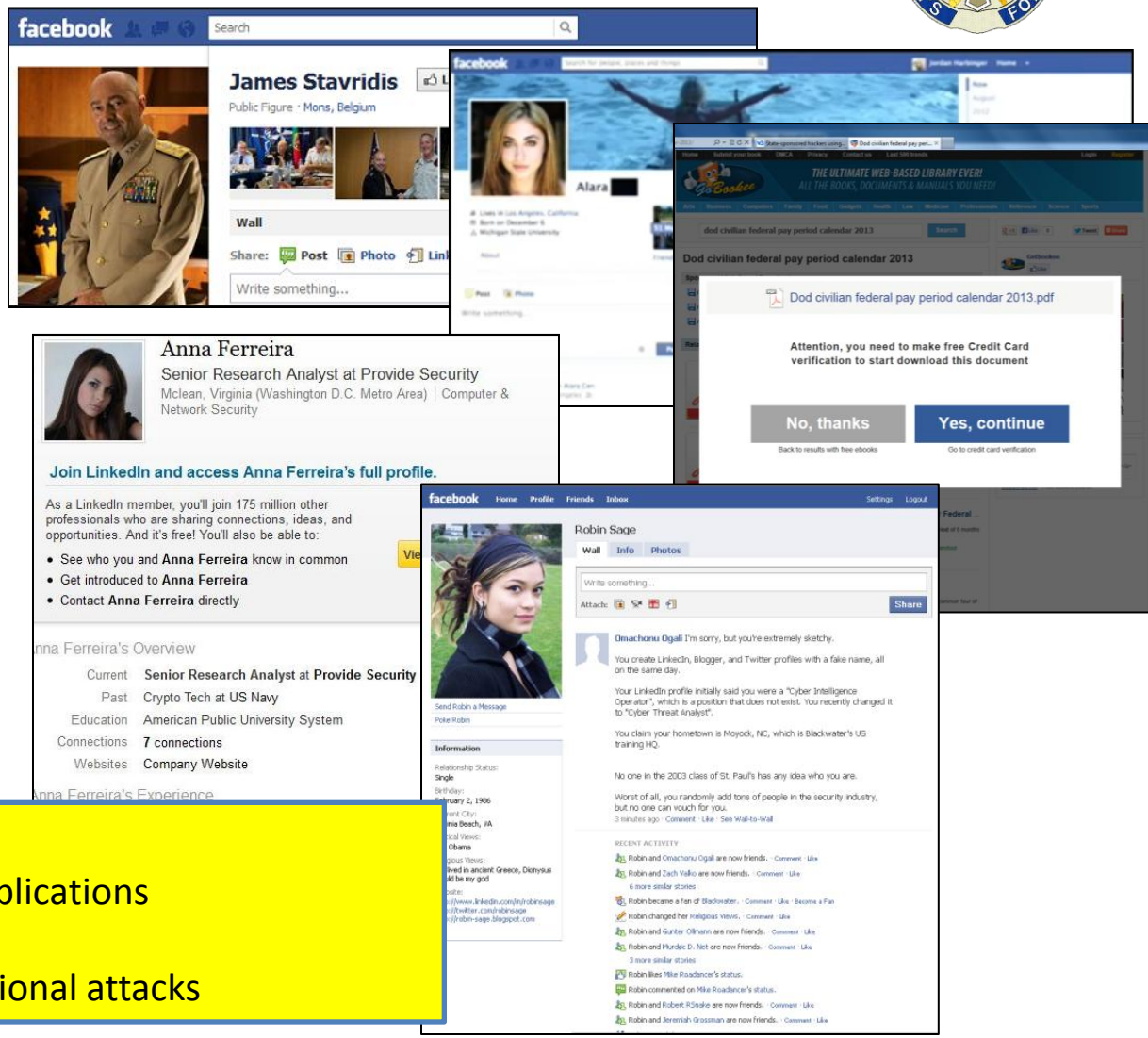
AFV decoy under Barracuda multispectral cam netting

Impact to the Warfighter:

- Loss of situational awareness
- Flood of fake targets – bogging down targeting process
- Expenditure of limited munitions on non-targets
- Negation of multi-spectral ISR assets (NVGs, IR scopes, EO)
- Negation of critical targeting planning and allocation of assets

“Electronic Decoys, Honey Pots, and Drive by Downloads”

- Decoys can represent a variety of personas on the Internet
- Some data repositories are also lures to
- Able to gain operational intelligence by posing as an individual with common interests
- Lures include social networking, job offers, and spoofed or fabricated PAO sites
- Can compromise personal data or release of malicious software



Impact to the Warfighter:

- Breaches in OPSEC can have real implications
- Puts professional reputation at risk
- Opens up the opportunity for additional attacks

Physical Destruction

Objective:

Destroys enemy's C^2 and information infrastructures (using systems approach to combat)

Target:

C^2 nodes and links, RISTA assets, telecommunication and power systems

"Attack the integrity of Information Communication Technology (ICT) systems"

- Threat will attack civilian ICT systems to demonstrate reach and deny friendly capability
- Threat is aware of friendly reliance on commercial ICT in theater
- Attacks could physical or electronic
- Much of the ICT upon which the US Government depends is under civilian control

Impact to the Warfighter:

- Bandwidth available to soldiers could be limited
- Soldiers could be required to revert to legacy pen and paper systems with little or no warning
- Combat critical reachback functions could be imperiled
- Communication capability degraded

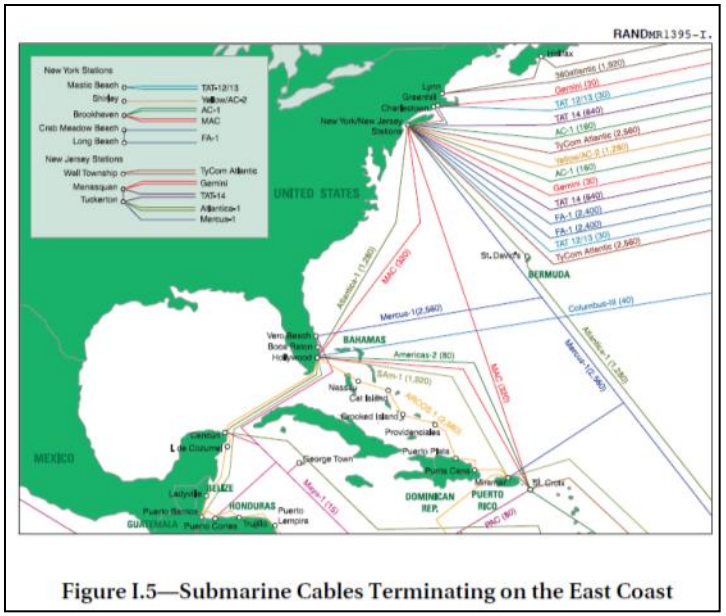


Figure I.5—Submarine Cables Terminating on the East Coast

Targeted attacks on submarine cables could result in a 95% loss in internet connectivity to/from the US

Protection and Security

Objective:

Protect critical assets and intentions

Target:

Enemy RISTA assets

"INFOWAR Counter Reconnaissance Capabilities"

- ***"Soft-Kill" capabilities incorporates electromagnetic jamming and computer warfare***
- ***Can counter friendly Computer Exploitation efforts through the use of electronic decoys, and all source analysis***
- ***Integrated into the Threat unit's fire support mission to counter early warning and target acquisition capability***
- ***Exploits poor OPSEC at JIIM Partners and logistics links***

A police officer shows how hacker attacks, struck the agency's headquarters.

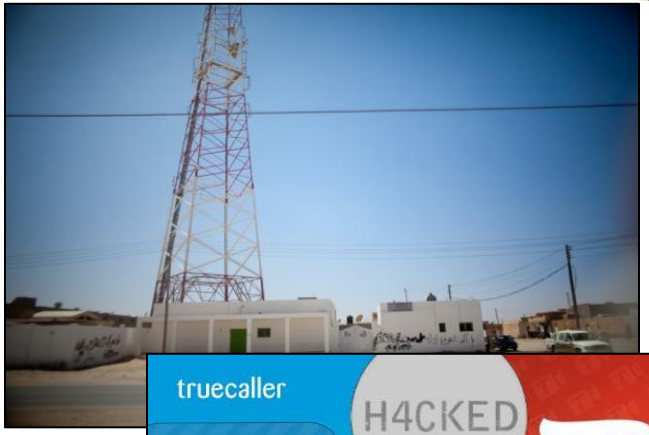
Impact to the Warfighter:
- Threat is persistent and requires constant vigilance
- Leaders of allied forces have compromised communications
- Little precedence establishing rules of engagement to provocation

Compromise Existing Civilian Infrastructure

- Threat will capture existing civilian infrastructure for intelligence purposes and C2 networks

- Hacked online directories used as a source for electronic surveillance and targeting

- Once control is established network becomes ad hoc C2 network



Impact to the Warfighter:

- Compromises links to host nation sources and support
- Achieves advanced threat C2, ISR capabilities by leveraging network capabilities
- Prevents information superiority by controlling access to telecom infrastructure

Perception Management

Objective:

Distort reality or manipulate information to support OPFOR goals and objectives

Target:

RISTA assets, media sources, populations, decision makers, commanders

"Disinformation False Messages"

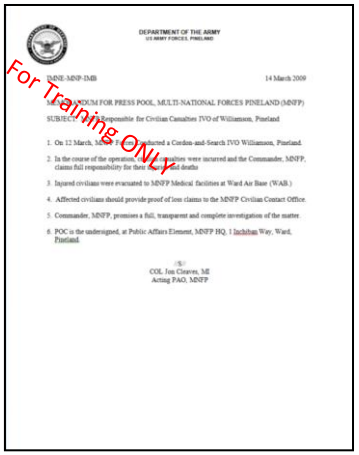
- Susceptibility to Disinformation is seen as a key US liability
- Such disinformation helps to drive Threat fundraising, recruiting and political efforts
- Threat uses civilian media to send official looking and sounding messages
- These messages range from mildly damning messages of US Army activities to false claims of responsibility
- Threat's understanding of local population increase acceptance of disinformation efforts

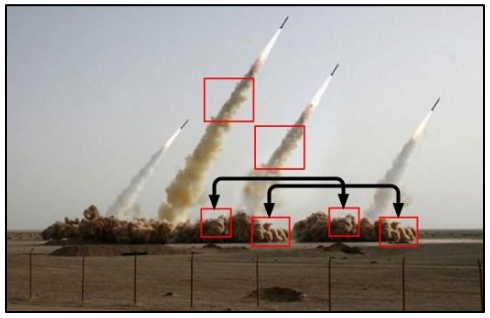
Impact to the Warfighter:

- Friendly commanders will be consistently behind the information cycle
- Intelligence cycle will be disrupted
- Friendly Commanders will often be tasked with de-conflicting and disproving false messages and disinformation
- Friendly soldiers will be forced to remediate the unwanted effects (civilian casualties, property damage, etc.) of attacks

Syrian Electronic Army hack
Associated Press Website.

False message implicating a friendly commander in civilian casualties





Iranian missile launch photo shopped to mask the misfire **of one of the TELs.**

“C2 via Social Media”

- Threat uses ICT such as SMS broadcasting to mobilize large numbers of protesters “Flash Mobs”
- Social media can function effectively as C2 mechanism civil unrest campaign and situational awareness
- Security forces require the same technology to operate thus shutting down the system is unfeasible
- The ability to communicate with one another makes the crowds more confident and willing to take risks
- Agitators sympathizers and bystanders are not easily distinguishable
- Activists will make up the core of future opposition groups and attempt to radicalize others through propaganda

Impact to the Warfighter:

- Unable to contain the mob and protect security assets at the same time
- Not easy to predict where the mob will strike next
- Can be used as a deception tactic to draw security away form intended target
- Unable distinguish between participants and bystanders

Flash Mob is dispersed by Police in London

Computer Warfare Information Attack

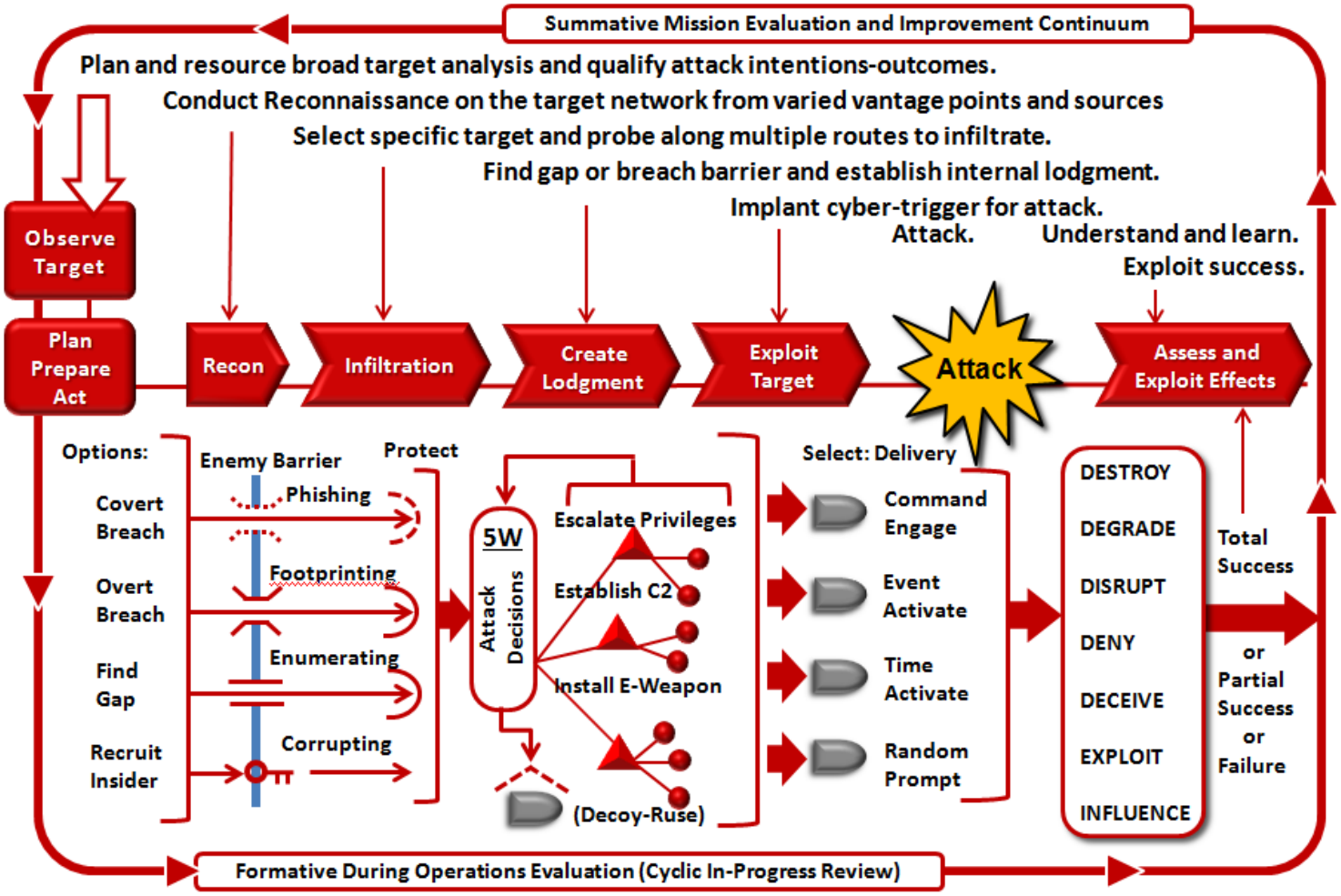
Objective:

Disrupt, deny or degrade the enemy's computer networks, systems and information flow

Target:

Command and control assets and networks (both civilian and military)

Cyber Attack Life-Cycle



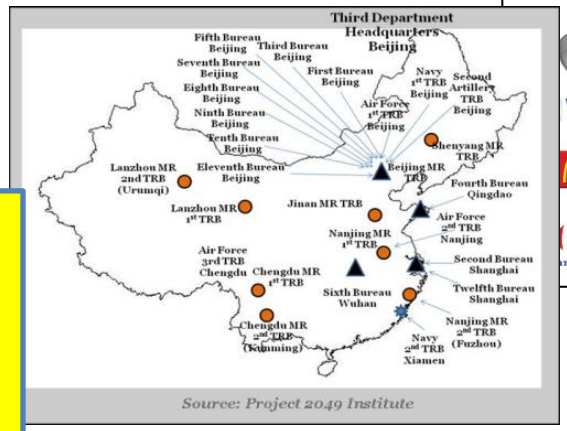
Advanced Cyber Reconnaissance and Surveillance Capabilities

Signature TTP: Information Attack, Advanced Persistent Threat (APT)

- ***Most comprehensive programs are state sponsored***
- ***Targeted attacks and APTs focus of organizations and individuals in a particular industry***
- ***Sophisticated attacks use social engineering techniques to obtain initial access***
- ***Developed persistent threat embeds into target system through malicious executable***
- ***Remote Access Tools are known as the AK-47 of offensive cyber operations and are used for C2 and monitoring.***

Hacker school.

Organizations with major breaches in security in 2012



Map of Cyber assets

Impact to the Warfighter:
- Persistent anonymous threat
- Strategic plans compromised
- Technical advantages mitigated
- Communications compromised by stealing messages

Nuisance Hacking

Signature TTP: DDOS, Defacement, Perception Management, Information Attack

- ***Included defacement of government and media websites***
- ***Re-purposes known Cyber security tools and techniques to penetrate target networks***
- ***Reroutes users to spoofed sites for exploit and attacks***
- ***DDOS attacks against financial, media and government institutions***
- ***Crossover of TTPs from Criminal elements***

Impact to the Warfighter:
•Lack of faith in host nation to provide information in time of crisis
•May impact ability to coordinate with other CF forces or HN due to networks downed by DDOS attack
•Can open CF personnel to compromised bank and credit card info

Websites run by the ""Cyber Army" offers downloadable attack kits with know exploits.

Georgian presidential website was defaced during the 2008 Georgian War

Syrian Electronic Army

“Malware Attacks”

- Attackers will use a variety of malware on Friendly computers to slow operations, extract data, or inject false data
- Poor operational procedures can enable this type of attack, with significant loss of capability and/or spillage of data to Threat Forces
- Recovery from an attack requires key assets and reduces operational effectiveness
- Malware could effect internal clocks (creating positional errors and communications difficulties) and slow the functional speed of computing
- Any internet capable or networkable system is at potential risk

Civilian Malware-removal software

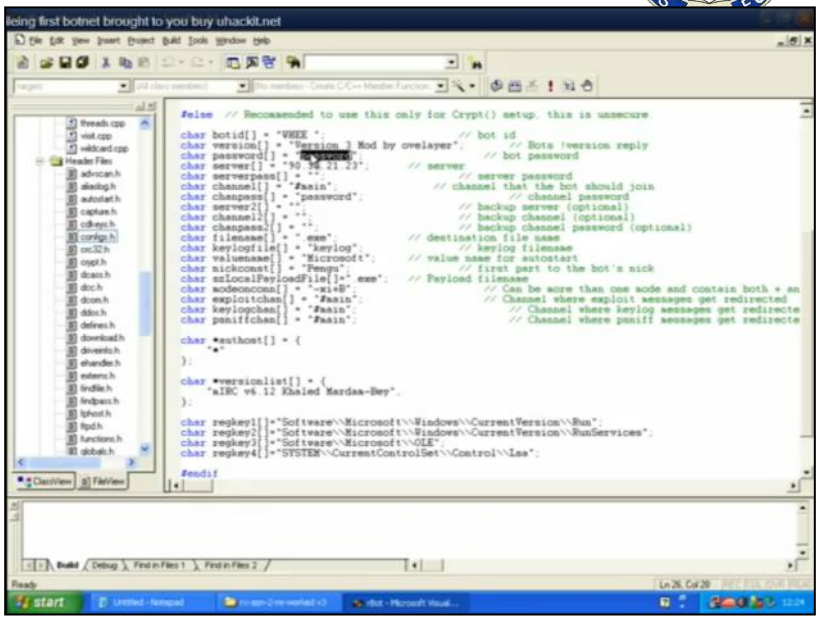
Potential targets

Impact to the Warfighter:

- Difficult to attribute attack
- Malware can cause creeping failures to imbedded systems like BFT, making identifying failures difficult
- Malware can be used to extract, destroy or manipulate data, software or the machines themselves

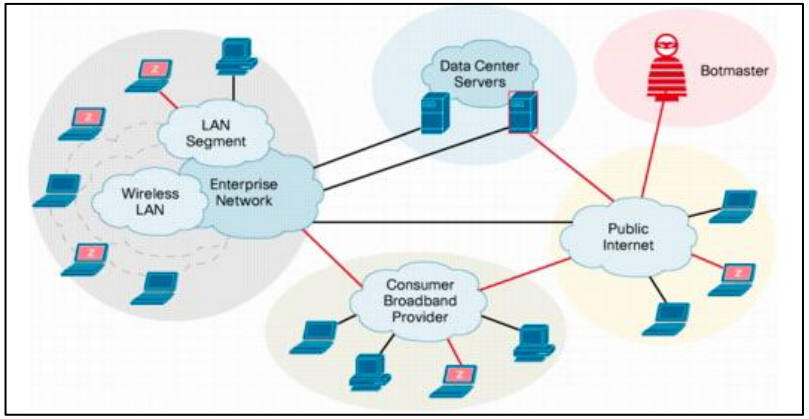
"DISTRIBUTED DENIAL OF SERVICE DDOS"

- DDOS attacks generally caused by thousands or millions of unwitting computers known as bots
- Establishes access through social engineering methods
- All computers with a public outlet to the internet are potentially vulnerable to this attack
- Represents a persistent threat that can be launched on demand
- Vulnerabilities include logistics and other essential military functions (communications, intelligence, and training)
- Telephones are similarly threatened by remote users
- Attack likely at strategic level with ripple down effects



Impact to the Warfighter:

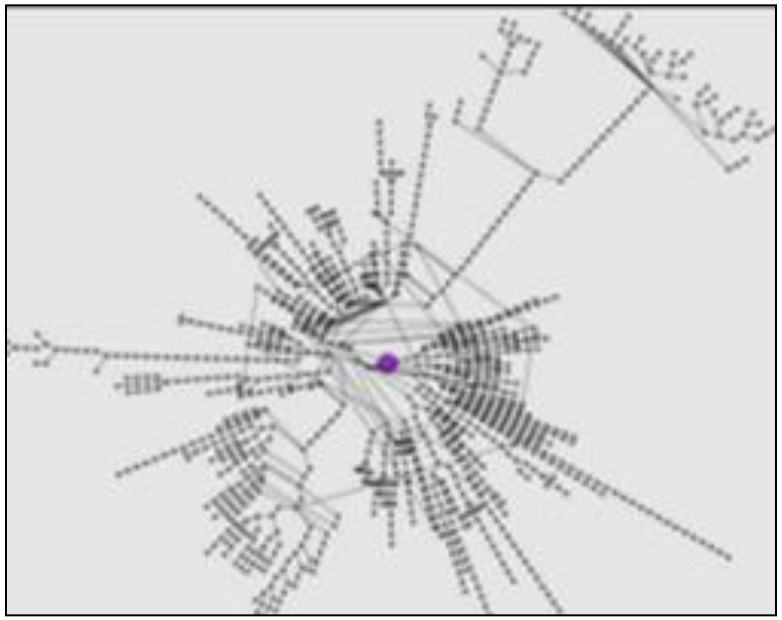
- Cause degradation and denial of basic services to the BCT at little cost to the Threat
- Can cause connectivity issues, including loss of NIPRnet-resulting in loss of NIPRnet functions like logistics, messaging, intelligence and administration
- Loss of network services could continue for hours or days



DDoS attacks at WIN-T links with larger networks can have tactical effects at engagement level

"Precision Computer Attack"

- ***Stuxnet: A cyber worm roughly 1MB in size***
- ***Used four (zero day exploits) to infect computer systems inside Iranian nuclear facilities***
- ***Targeted explicit system requirements based on hardware and software criteria before release of payload***
- ***Used vectors like USB drives instead of the internet to infect systems in an "air gapped" digital environment***
- ***Established a peer to peer network with other infected systems for updates and C2***



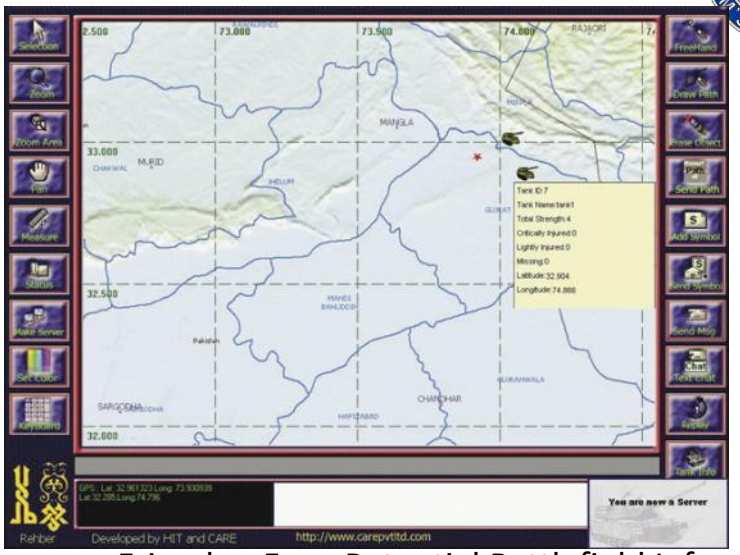
Stuxnet's propagation mechanisms are all LAN based and thus, the final target must be assumed in close network proximity to the initial seeded targets. Source: W32.Stuxnet Dossier www.symantec.com

Impact to the Warfighter:

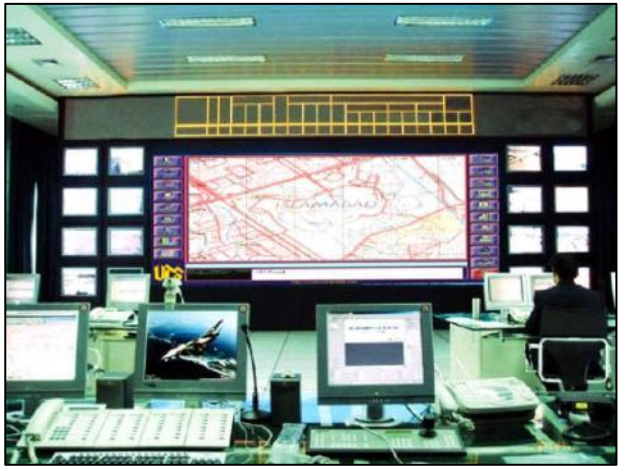
•Even Air gapped systems are at risk due to poor OPSEC
•Attack based on intimate knowledge of the Iranian nuclear system of systems
•Potential for attack victim to propagate the attack by repurposing executables

"Disinformation in Trusted Networks"

- Threats will attempt to inject disinformation through trusted networks
- Threats will attempt to make Friendly distrust their ISR and Situational Awareness assets like Battlefield Information Management Systems by injecting incorrect information
- Attacks could take the form of icon shifting (blue to red) or moving the icon's location
- Fire missions and unit control would require significant human interaction, thus slowing Blue's target engagement cycle time
- While BFT has significant hardening against this type of



Friend or Foe: Potential Battlefield Information Management System uncertainity has tactical implications.



Impact to the Warfighter:

- Reliability of Battlefield Information Management Systems in doubt
- MDMP negatively impacted – loss of data integrity, prolonging planning cycles
- Possible Friendly Fire events
- This attack would force Friendly onto legacy Mission Command systems with which training and proficiency would be minimal or non-existent

Information Warfare in Training

- Free Play, Free Play, Free Play
- Deception
- Degradation of Capabilities
- Non-Combatant Response

Questions?