Cyber-warfare

(2nd lecture)

The dark side of ICT

Gian Piero Siroli, Physics & Astronomy Dept. Univ. of Bologna & CERN

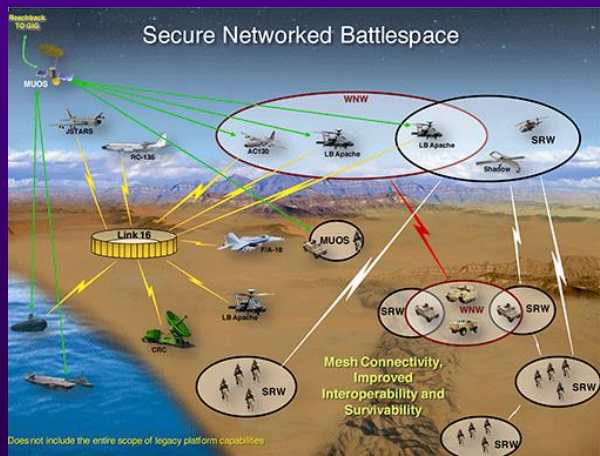
CERN Academic Training, Geneva, January 2016

A different view on cyber-war

- Threat to military systems
  - **Vulnerability of weapon platforms: increasing dependence on s/w intensive systems (h/w manufacturing, firmware), communication & control systems, sensors, battlefield networking. Automation. Embedded computing in military applications**

    - Advanced aircrafts: >75% of performance & capability dependent on s/w. F-16 unstable below mach-one, uncontrollable without s/w based flight control. Boing-777 & Airbus-330 s/w flight control without manual backup. F-22 cyber-controlled aircraft: not a closed system, external information systems update & integrate combat ops during flight, possible attack to s/w & h/w sys of F-22. F-35: ~10M LOC

  - **Cyber infiltration of C4ISR systems. Battle management: disruption of military communication & coordination**
  - **Drones & unmanned systems (UAV, UGV, UUV)**
- Battlefield digitization
  - **Airborne networks for communications. Bridging technologies (Link-16, Link-11, Link-22 etc) to exchange tactical picture in near-real time, situational awareness, coordination of weapon systems. SDR**
  - **High speed networks for live video feeds, image, voice & sensor data transfer/processing, battlefield surveillance, C&C. Mobile "ad-hoc" & sensor networks**



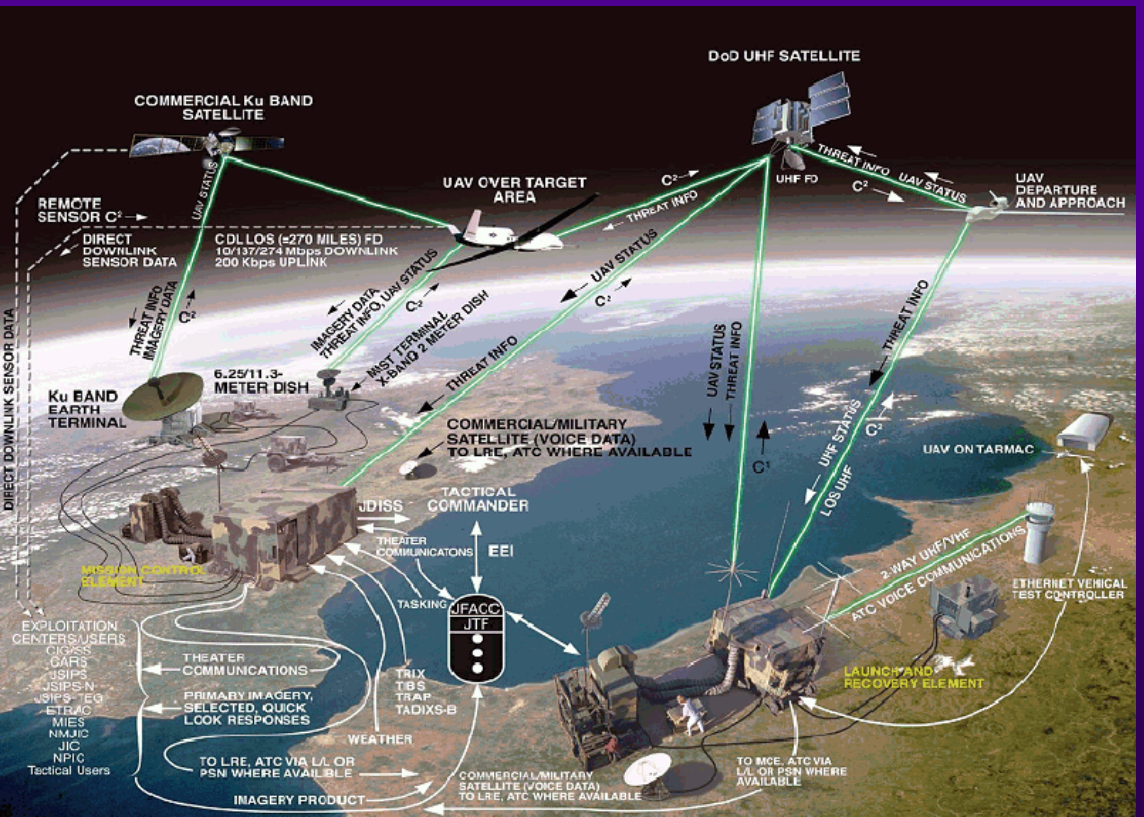

NATO OTAN

F-35 cockpit

US Navy unmanned 11-meter rigid hulled inflatable boat (RHIB) from Naval Surface Warfare Center Carderock, as it operates autonomously during an Office of Naval Research demonstration (Associated Press)

Global Hawk UAV

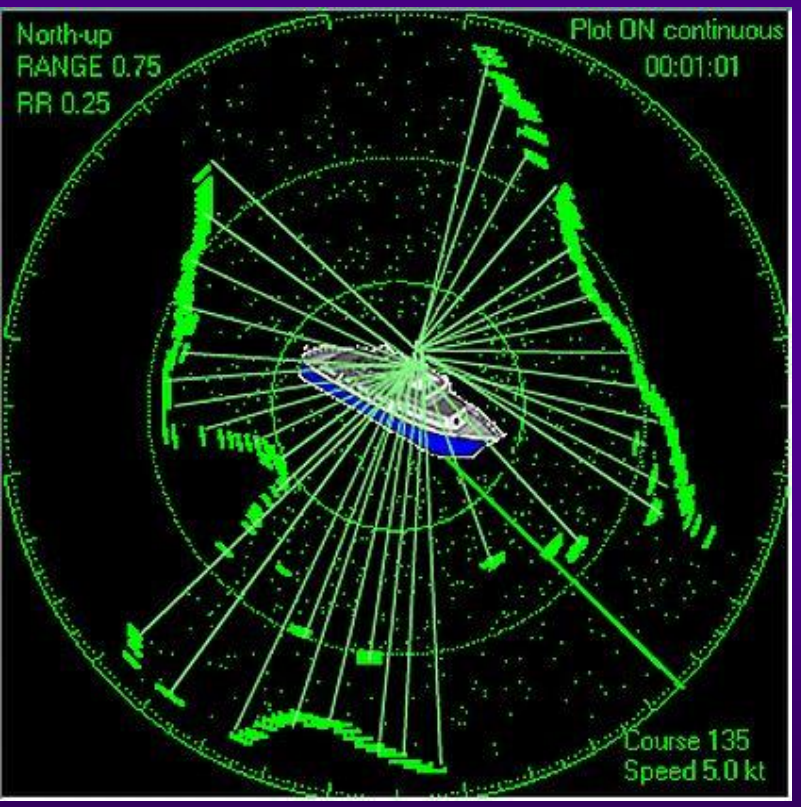
- Continuous day/night, high altitude, long endurance, all weather surveillance & reconnaissance in direct support of ground and air forces, sensor data to tactical units. Strike. Visual, IR, SAR imagery. Intelligence gathering, terrain obs, targeting. (UGV, UUV)
- Integrated system: mission control (plan, C&C, communications, monitoring), launch/recovery, vehicle tests



- Hardware attacks during maintenance/storage: corrupt data stored on board, install extra components
- Remote cyber attacks during ops through comms: alter data on board (vehicle/system state, navigational, C2), break encryption of comm channel
- Sensor spoofing: GPS spoofing, blind vision sensors
- Buffer ovfl through some input device, event triggering, forced sys.reset, malicious code & packets, overload & DoS CPU/controllers…
- Dependence on uninterrupted comms: failures/accidents due to environmental EMI, EW threats, jamming

Digitally programmable adaptive radar

Adaptive radar uses digital technology to change its characteristics dynamically to adapt to changes in its environment. In particular, adaptive radar is being designed to counter the effects of EW countermeasures and other RF interference



Today's airborne EW systems are proficient at identifying analog radar systems that operate on fixed frequencies. Once they identify a hostile radar system, EW aircraft can apply a preprogrammed countermeasure technique.

Digitally programmable radars have unknown behaviors and agile waveform, so identifying and jamming them is becoming increasingly difficult.

Adaptive Radar Countermeasures (ARC) need to generate effective countermeasures automatically against new, unknown, or ambiguous radar signals in near real-time

Electromagnetic spectrum sharing among radar & communications systems

RTR8GE secure battlefield router for mission-critical communications and information sharing (GE & Juniper Networks)

Insatiable demand for bandwidth and onboard processing capability in UAV platforms

US Cyber Command: solicitation released to provide mission support services in cyberspace operations, cyber planning, all-source intelligence, cyber training & exercises, project management, policy, security, and other cyber support services ($460M)

Cyber-warfare "products"

Hacking Team

- IT company selling offensive intrusion/surveillance capabilities to monitor coms, decipher encrypted files/emails, record Skype & other VOIP coms, remote activation of microphones/cameras & record audio, keystroke logging, rootkit infection etc
- 2014: HT exports frozen by IT gov (human rights concerns), then released
- 2015: Data breach (400GB) of platform tools & customers, mostly military, police, governments
- s/w suited to support military ELINT ops, potentially falling under the category of 'military equipment' (UN panel on selling to Sudan)

FinFisher (by Gamma Int.)

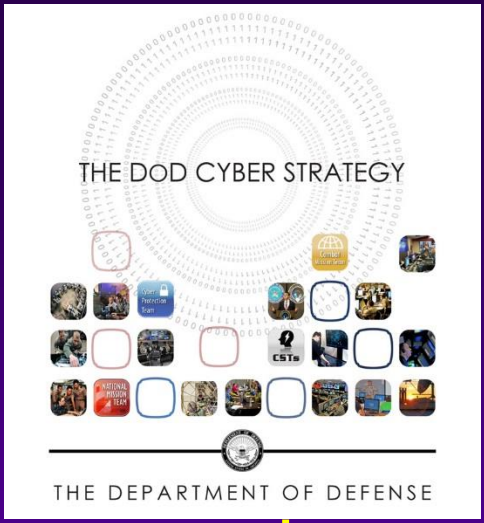
- Spyware suite sold exclusively to govs for intelligence and law enforcement purposes
- Marketed as a tool for fighting crime, FF involved in surveillance abuses. Bahrain's government used FF to monitor some of the country's top law firms, journalists, activists, opposition political leaders. Ethiopian dissidents in exile
- Attacked as HT

¿ Cyber-war ?

- ’80s - Siberia: pipeline explosion
- ~2000 - Serbia: ICT attack on air defense system, Iraq: attack on banking and telephony networks
- 2005 - Greece: ICT intrusion in mobile communication system by foreign intelligence
- USA: various electrical blackouts on a regional scale by cyber attacks
- 2007 - Estonia: prolonged attack against many national organizations (finance, public administration, media)
- 2008 - Syria, Georgia: cyber attack targeting air defense system and C&C centres in support of conventional operations
- 2009 - USA: video feeds of drones (Iraq) intercepted
- 2010 - USA: unified Cyber Command (CYBERCOM)

STUXNET

US DoD cyber strategy



- Primary missions:
  - Defend DoD networks, systems, information
  - Defend the US homeland & national interests against cyberattacks of significant consequence
  - Provide cyber support to military operational and contingency plans

- Building bridges to the private sector and beyond. Attract best talent, ideas, technology
- Deterrence key part of cyber strategy
- Build & maintain ready forces & capabilities to conduct cyber ops & control conflict escalation
- Build international partnership to deter threats and increase security & stability

Cyber-war actors

- Governments: armed forces, intelligence services
- Large organizations and structured networks (legal & illegal)
  - Large private companies with vast resources
  - Organized crime: financial frauds, online banking transactions, economic espionage, communications (cyber-crime)
  - Specialized organizations serving governments (cyber-mercenaries)
- Hackers / hacktivists
- Insiders
- Many different actors (state & non-state), diverging interests

Comments on cyber-war

- Most dangerous parts of Stuxnet are generic, not specific to uranium enrichment plants, can be copied and modified to work in different environments. Delivery in different ways than USB sticks (remember Code Red). Discovered executables using (parts of) Stuxnet source code
- Cyber is a “once-only” weapon (lost after delivery)? Cyber-weapons proliferation?
- Probably many countries have technology and skills to initiate cyber attacks. Cyberspace already militarized, digital arms race?
- Cyber-war <- Battlefield digitization <- Electronic Warfare

  ICT & microelectronics (r)evolution in warfare techniques and battlefield (sensors, computers, telecommunications, data processing systems). ICT (dual use technology) inter-domain underlying layer (cyber->anywhere)

Comments on cyber-war

- Cyber is an autonomous operational warfare domain. Cyber-only-war will probably never exist
- Is "cyber" different from land, sea, air, and space warfare operative domains? Artificial dimension created by man. Cyber-space is both a weapon AND a target at the same time?! Space/topology of the weaponry can be affected by the weapon (like if weapons used in warships could change the geography of oceans). Cyber-topology VERY volatile: regions of cyberspace appear/disappear on command or under (cyber/conventional) attack. Different "geography" from different locations
- Asymmetric war: dependency on vulnerable complex infrastructures. Asymmetry of actors, costs and vulnerabilities. Technological dependence on h/w (f/w) & s/w producers
- Wide and inter-disciplinary domain (technical, socio-political). Need to develop a new global vision/vocabulary
- Conflict & pre-conflict activities (PSYOPS)

Specific features of cyber-warfare
(mixing of strategic, operational and tactical levels)

- Mobility of cyber-weapons (worms), propagation speed very high. Maneuverability
- Striking power, fire capacity: volume, range, speed at which cyber-operations can be conducted. Definitions? Comparison with conventional domains?
- Network interconnections/integration, (near) real-time system (ability to successfully engage time-sensitive targets anywhere in the world). Sensor to shooter: integration with battlefield sensors systems/platforms
- Very high level of automation. Automation of C&C (decreased time from identification to engagement). Cyber RoE (man-out-of-the-loop)? No need to enable cyber-weapon, just release it on the net. Automatic target search/guidance (or logic conditions to trigger payload), “Fire and Forget”

Specific features of cyber-warfare

- Fast global communications (situational awareness). Large amount of data (battlefield digitization)
- Defense/protection (of weapons and network/territory)? Attack?
- Territorial (i.e. network) characteristics: territorial penetration/destruction. Territorial control/denial?? Is network/territory valuable? Geography (network topology) under human control and vulnerable, very mutable environment, dynamically created and destroyed. Limits? Vulnerability/domination of chokepoints (rapidly changing). Operations in hostile environment
- Offense dominance!? Offense (destabilizing, first/preemptive strike) VS defense (stabilizing) balance. Cyber precursor of conventional attacks? High cost of defense, effectiveness?

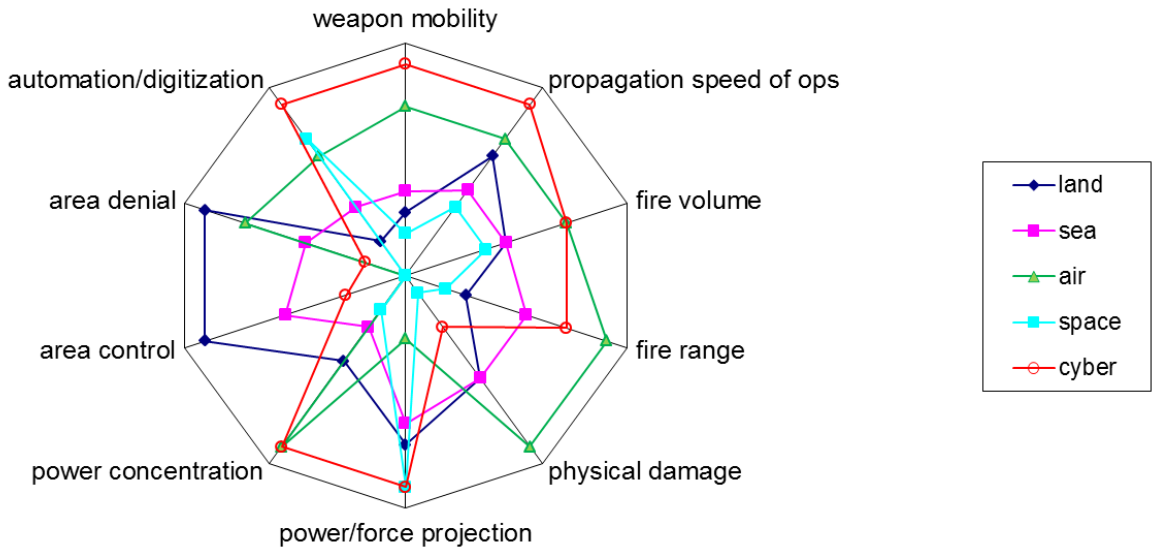
Specific features of cyber-warfare
(strategic level)

- Deterrence (nuclear age concept) applicable to a cyber-weapon system?? Deterrence by retaliation complicated by attribution problem (difficult direct identification of attacker, at geopolitical level?!). MAD at cyber level?!
- When a cyber-attack can be considered an "act of war"? Limits in peacetime? Right to respond with traditional kinetic options: "The US reserves the right…to respond to serious cyber attacks with an appropriate proportional and justified military response". Definition of cyber-attack?
- Changeability
  - Technological: very rapid deployment of new technologies (time-to-battlefield). Fast technological development can change the nature of cyber-power?
  - Human: expertise increase slowly over time

Specific features of cyber-warfare
(strategic level)

- New source of intelligence
- Is verification possible (agreements/treaties) in cyber-domain? Detection difficult. Cyber-weapons control??
- "Cyber" best for? Guerrilla-like operations? Intelligence, sabotage, single time-limited/highly targeted attacks? Support to conventional operations? Short or long term advantages? Consequences on other warfare domains (digitization, structures)?
- Integration/predominance of X-warfare (land, air, sea, space, cyber)? Is global stability increased or decreased by adding one more dimension?
- Man "in", "on", "off" the loop

Warfare domains comparison



A flash on a wider perspective on military strategy

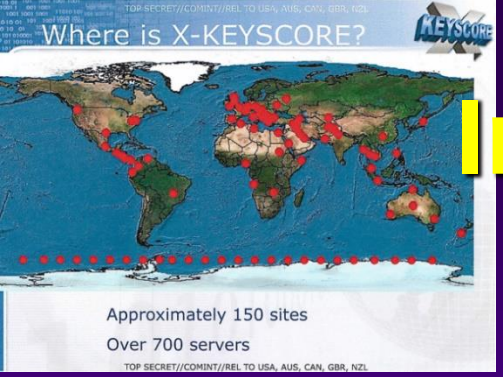
How does cyber fit in military strategies?
A new warfare domain modifies high level strategies?

- **Sun Tzu (~500BC): low level of violence, preparedness, stealthiness, intelligence (Stuxnet?)**
- **C.von Clausewitz (~1800): any act of war has to have the potential to be lethal, instrumental, and it has to be political (does cyber fit?)**
- **G.Douhet (~1900, visionary): air-power revolutionary operating in 3rd dimension, proponent of aerial strategic bombing. Vital center destruction. Basic targets: industry, transport infrastructure, communications, government and "the will of the people". entire population in the front line. Total war concept (very relevant)**
- **Technological evolution: sea-power, tanks, air-power, cyber. RMA(?)**

Information Warfare e PSYOP

- Internet as a global communication "medium"
- Information Operations (IO): info manipulation for (counter)propaganda, disinformation, consensus building, discrimination, defamation, delegitimation, censorship/content filtering. Deception, perception war, influence ops. Traditional techniques on a new medium. Counterintelligence, ops security

  "Nihil est quod videtur" "..Cicero.."
- Real world examples: support to dissident groups, recruitment campaigns, use/manipulation of social media/networks. Wikileaks, NSAleaks, EZLN
- Network is an ubiquitous surveillance environment
- Info war: primary political (strategic) value. "cyber influence" might contribute to political and social instability of a country. Blurring distinction between military and civilian domains



Inside TAO NSA hacking unit

- It maintains its own covert network, infiltrates computers around the world, intercepts shipping deliveries to plant backdoors in electronics ordered by targets. Acquisition of former Sony chip factory. Exploitation of technical ICT industry weaknesses
- Computer Network Exploitation on every type of devices: servers, workstations, firewalls, routers, handset, phone switches, SCADA systems. BIOS level for persistence. Probably ~85000 nodes infiltrated worldwide. NSA shadow network with “covert” routers & servers including non-NSA infected devices
- “Xkeyscore”: fish crash reports over the net. >700 servers at ~150 sites where data is collected. searching and analyzing global Internet traffic
- “Angry Neighbor, Howlermonkey, Waterwitch”: implants of a large number of Trojans spying tools
- “Quantum”: sophisticated toolbox to perform attacks in a largely automated way (IP addr, AOL, LinkedIn, Youtube, Twitter, Hotmail, FB, Gmail, Yahoo …..). On the market!?!

GCHQ surveillance and propaganda

- Set of exploit tools from JTRIG (Joint Threat Research Intelligence Group), a unit of the British GCHQ
- UK MoD secret, multimillion-pound research program into the future of cyber-warfare, including how emerging technologies such as social media and psychological techniques can be harnessed by the military to influence people's mind and beliefs
- “Miniature Hero”: Active Skype capability. Provision of real time call records and bidirectional instant messaging
- “Hacienda”: scans open ports on all public servers to seek out vulnerabilities (~30 different countries scanned). ORBs
- “Scrapheap Challenge”: perfect spoofing of emails from Blackberry targets. “Underpass”: Change outcome of online polls. ”Gestator”: amplification of a given message, normally video, on popular multimedia websites (YouTube)

What about privacy & human rights??

International Framework

- First steps: define cyber-war context and scope, evaluate interdependence between CI and vulnerability/risk level (anomalies, interferences, cascade effects). Collect infos from private and public sectors. Creation/coordination of national agencies, development of legislation, cyber-security awareness campaigns
- Bilateral and multilateral initiatives. Many institutions: UN, ITU, OSCE, G8, EU, NATO. UN resolutions since 1998 "Developments in the field of information and telecommunications in the context of international security". Still need to define basic concept of info-security and international principles (1999). "Creation of a global culture of cyber-security and the protection of critical information infrastructures" (2004). UNIDIR (1999, 2008)
- In the past: limited international cooperation followed by end of dialogue. More recently: perspectives for a more open debate (even with different focus). Forum for agreements?

UN agenda

"Developments in the field of information and telecommunications in the context of international security"

Annual reports by Secretary General to GA:

- **2015: A/70/172. Reports by Canada, Germany, Mozambique, Netherlands, Qatar, Republic of Corea, Spain, UK**
- **2014: A/69/112, A/69/112/Add.1. Reports by Canada, Colombia, France, Georgia, Germany, Republic of Korea, Serbia, Spain, Sweden, UK**
- **2013: A/68/156, A/68/156/Add.1**
- **2012: A/67/167. Report by Germany**
- **2011: A/66/152, A/66/152/Add.1**
- **2010: A/65/154**
- **... Back since 1998 (A/RES/53/70) draft resolution by Russia**

Four Groups of Governmental Experts (GGE) examined existing potential/threats from the cyber-sphere & possible cooperative measures to address them (A/65/201 2010, A/68/98 2013, A/70/174 2015). New GGE in 2016/17

UN agenda

“Developments in the field of information and telecommunications in the context of international security”

GGE in 2014/15:

- In their use of ICTs, States must observe State sovereignty, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States
- Existing obligations under international law are applicable to State use of ICTs and States must comply with their obligations to respect and protect human rights and fundamental freedoms
- States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts
- UN should play a leading role in promoting dialogue on the security of ICTs in their use by States, and in developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour

“The right to privacy in the digital age”, A/RES/68/167 (2013)

Some initiatives - I

- Trusted identity on the net (nodes, users, processes). Development of mechanisms of authentication, identification, digital certification. Data integrity, confidentiality, availability. Cryptographic techniques. Currently high(?) level of anonymity. Problems(?) with traceback for attribution. Public disclosure of 0-day vulnerabilities? Privacy??
- Creation of international warning centers and support to cyber emergencies/accidents. Distributed sensors (already existing in private world)? Institutions for investigation or/and forensic analysis?
- Effective collaboration/cooperation between public and private sector (diverging interests). Define responsibilities. Pilot programs to define regulations, incentives, political-economic schemes. Resilience

Some initiatives - II

- **Cyber-war (technical vision) VS Info-war (content). Privacy, freedom of expression, civil rights**
- **Development of a clear international legal framework: *jus ad bellum* and *jus in bello*" (discrimination and proportionality, military and civilian targets, neutrality, collateral damages). Is cyber-attack an act of war? Creation of mechanisms to harmonize legal issues in national legislations. Cyber domain probably the least regulated warfare domain (no specific regulation at all) compared to traditional warfare domains (land, air, sea, space)**
- **Cyber-security: global (asymmetric) issue crossing individual national borders. Total protection impossible. Unavoidable international cooperation?! Collective security!? Global vulnerabilities!!**
- **At national level: strategic planning to formulate a coherent domestic doctrine. Integration with traditional warfare domains. Coordination of national agencies**

Final Notes

- «Cyber universe» new warfare domain, constantly changing environment, artificial, extremely volatile, not well defined. Could it change/reduce the distance among main actors in the international arena, at least partially or temporarily? ≈>40 countries developing cyber offensive capabilities
- Will main military powers dominate also this new dimension? Change balance of power? Asymmetric characteristics may reposition less technologically advanced countries or alter dynamics of global power?
- Future conflicts will have a cyber dimension (hard or soft) currently difficult to evaluate. Number of actors and operational capabilities will increase. Man “in”, “on“, “out” of the loop. Hostile activities taking place during peace time
- ICT-based approach will not be sufficient: human, organizational, political and economics factors will have to be considered (consequences of outsourcing, deregulation practices, privatization). Cyber supply chain
- Cyber-weapons control?

What is happening now

- The US Obama administration shows openings for bi-multilateral discussions (UN, ASEAN Regional Forum (27 countries), G20, OSCE, ITU with only technical role?) and cooperation in cyber-security. Previous US administration almost completely locked. 2013 very active year: bi-multilateral contacts USA, Russia, China, ARF [written in 2013].

  2013: US-Russia cyber-hotline for proactive mitigation of threats

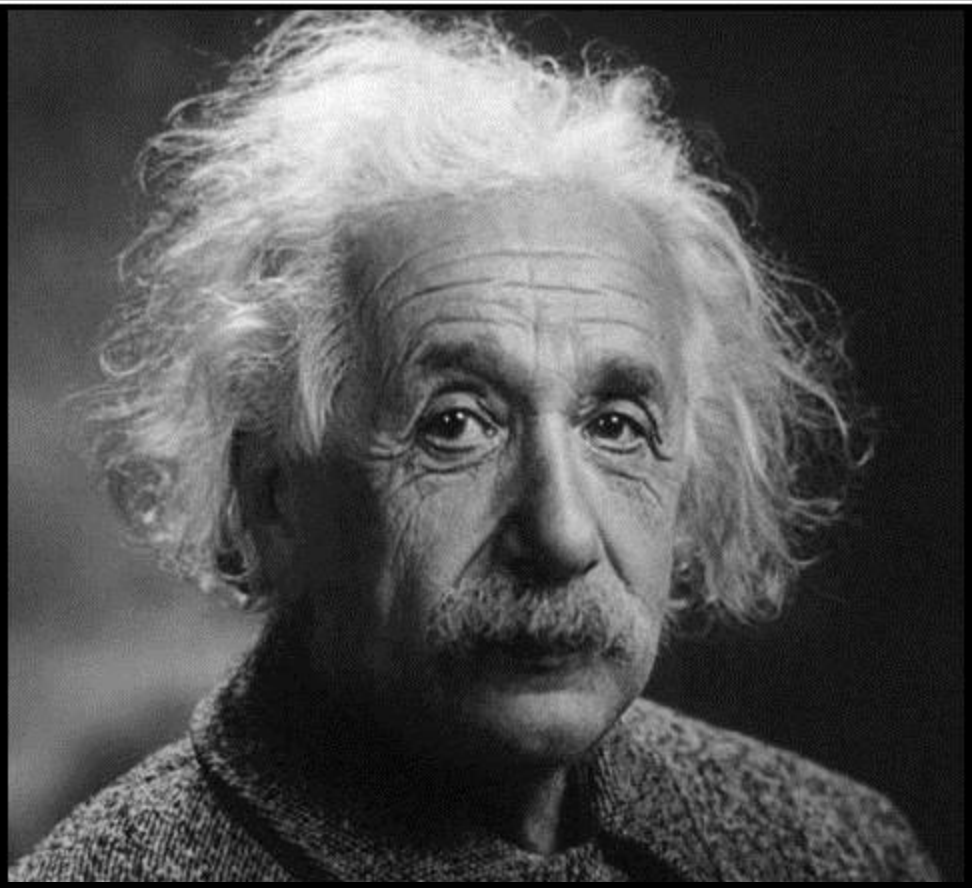
  …then 2014 Russia-Ukraine crisis (&NSALeaks in 2013)…

US-Russian Cooperation on Information & Communications Technology Security

- Deepening Engagement through Senior-Level Dialogue
- ICT Confidence-Building Measures
  - Links between Computer Emergency Response Teams
  - Exchange of Notifications through the Nuclear Risk Reduction Centers
  - White House-Kremlin Direct Communications Line

other domains)

- If states feel vulnerable self-restraint on cyber-weapons is mutual interest?! Collective self-defense? Risk of escalation. Focus on stability. Fast tech innovation, slower diplomatic cycle
- Verification portion of any cyber-control agreement extremely problematic. Malware production regulation impossible?! Reaching agreement on rules limiting behavior. Assistance to states under attack. Important to start a process

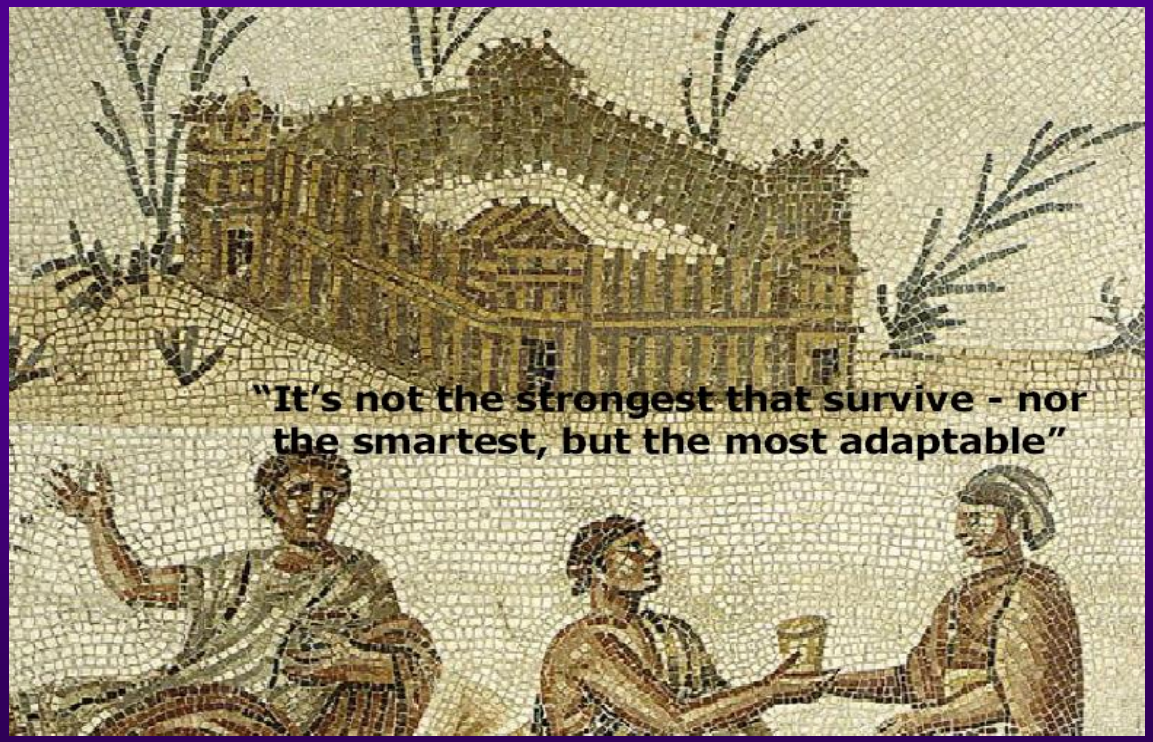


Solution is not at the ICT technical level only

“We cannot solve problems by using the same kind of thinking we used when we created them” A.Einstein

“Attaining one hundred victories in one hundred battles is not the pinnacle of excellence. Subjugating the enemy’s army without fighting is the true pinnacle of excellence”

Sun Tzu, The Art of War, about 500 BC




LIFE AFTER ICT

Real time cyber attacks world map

http://map.ipviking.com/?_ga=1.106938115.1477390587.1388686673#

http://map.norsecorp.com/

https://cybermap.kaspersky.com/

http://www.sicherheitstacho.eu/?lang=en

https://www.fireeye.com/cyber-map/threat-map.html