IDEAS THAT WORK FOR
INDUSTRIAL
DEVELOPMENT

Cyber Warfare 4.0 meets Electronic Warfare Opportunities and Implications

Dr Jabu Mtsweni
CSIR Research Group Leader: Cyber Defence

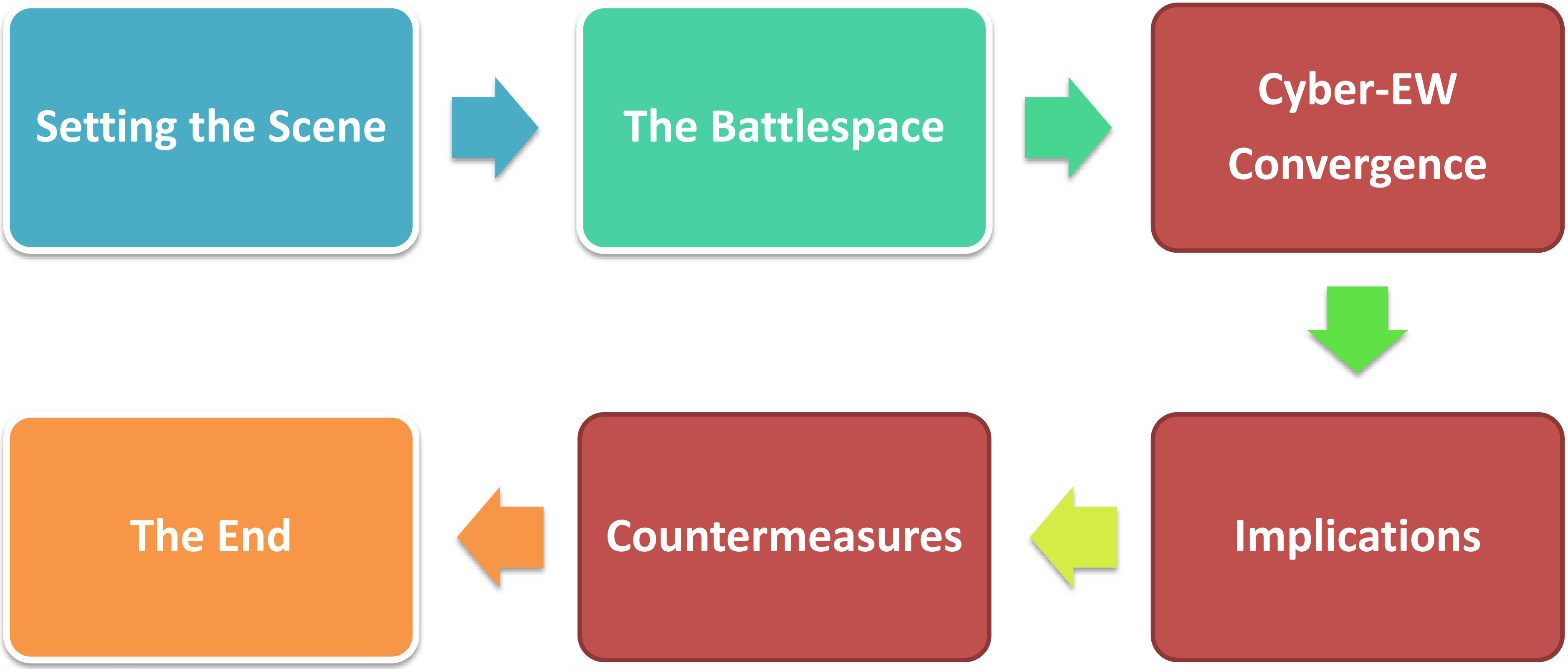
ELECTRONIC WARFARE SOUTH AFRICA 2017
International Conference & Exhibition
6-8 November 2017 | CSIR, Pretoria

CSIR
our future through science

Disclaimer

- The views or opinions expressed in this talk are not that of my employer (CSIR).
- All images used in this presentation belong to their respective copyright holders, unless otherwise stated,
- All images are used for non-profit educational purposes in accordance with Fair Use Copyright laws.
- This presentation is available for sharing without any prejudice

Presentation Outline



Setting the Scene

The Battlespace

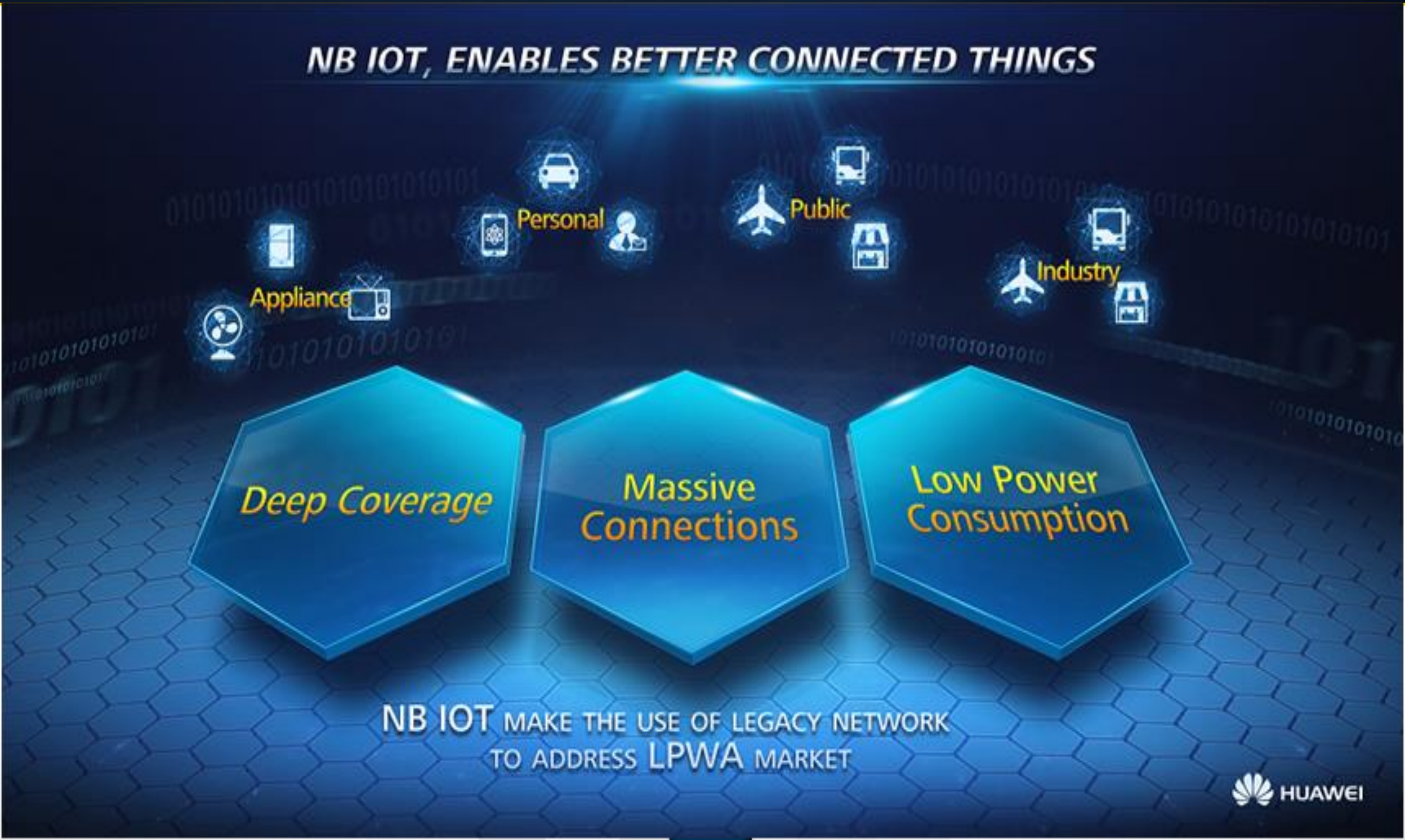
Cyber-EW Convergence

Implications

Countermeasures

The End

New Connections in the Hyper-connected World



NB IOT, ENABLES BETTER CONNECTED THINGS

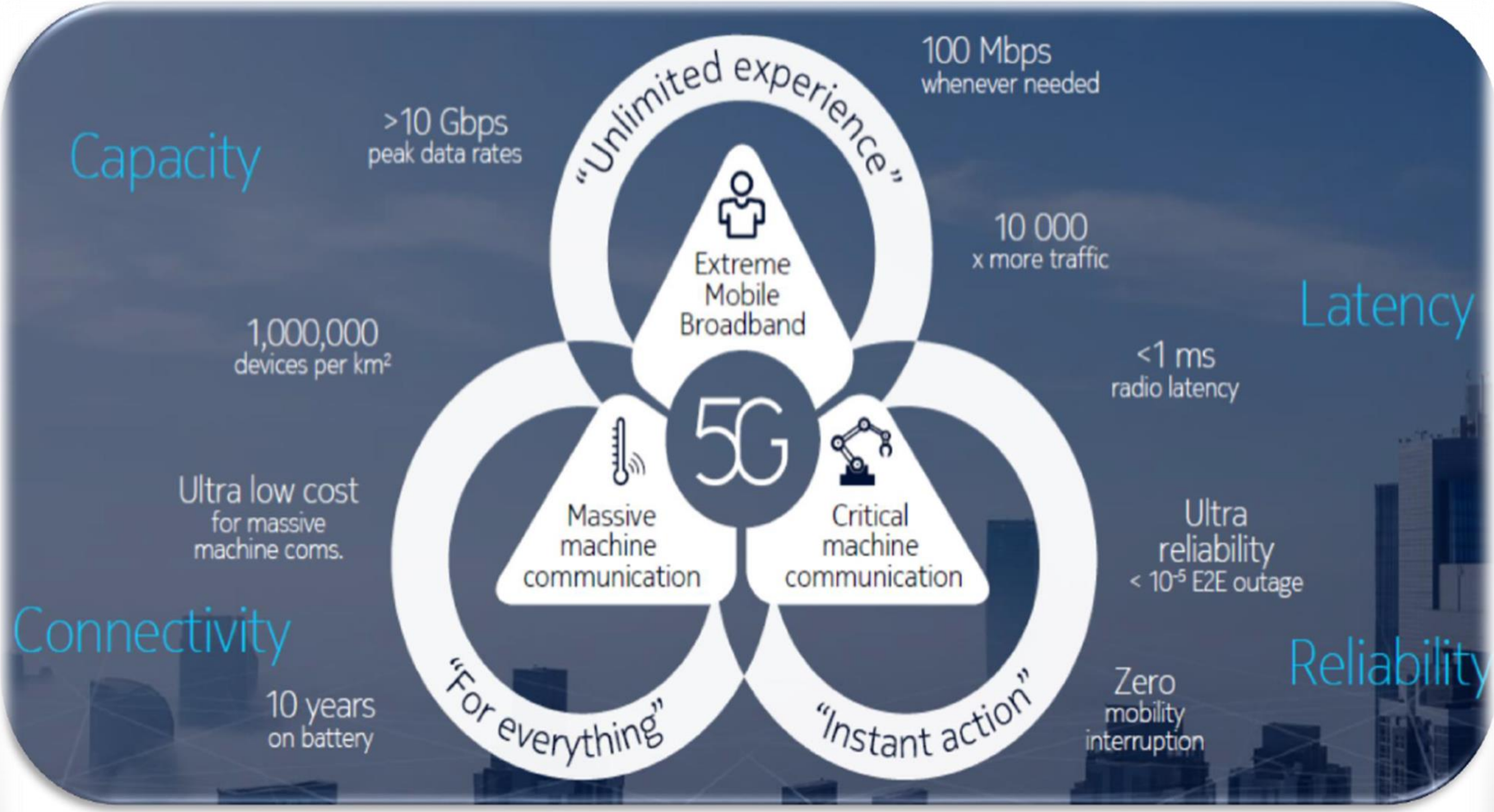
Deep Coverage

Massive Connections

Low Power Consumption

NB IOT MAKE THE USE OF LEGACY NETWORK TO ADDRESS LPWA MARKET

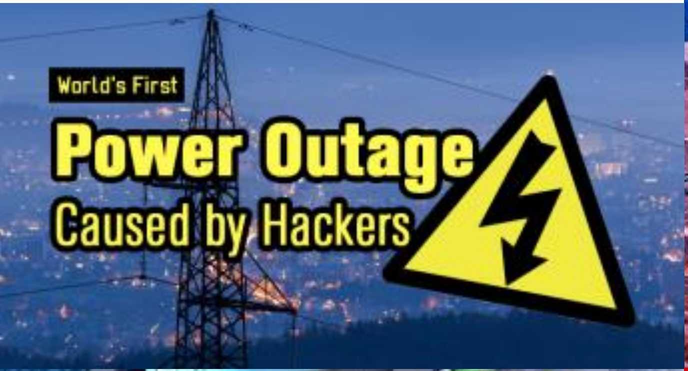
Diversity of Networks…

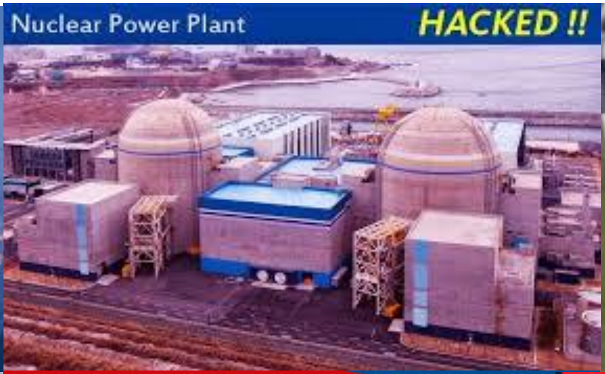


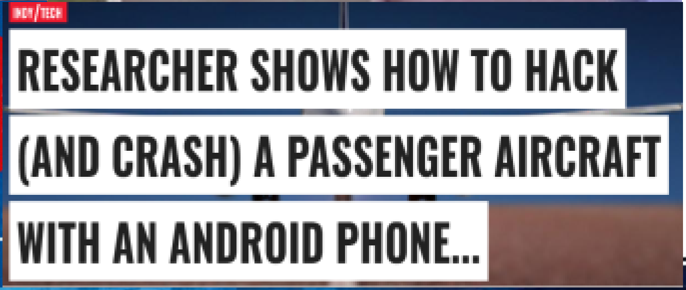
Courtesy of Nokia

The increase attack surface

- Cars have been hacked, a popular U.S. smart home alarm system was hacked, implantable medical devices like pacemakers have been hacked, plane systems have been hacked, critical infrastructure like a power grid and a dam were hacked, mobile banking apps have been hacked, smart city technology has been hacked.

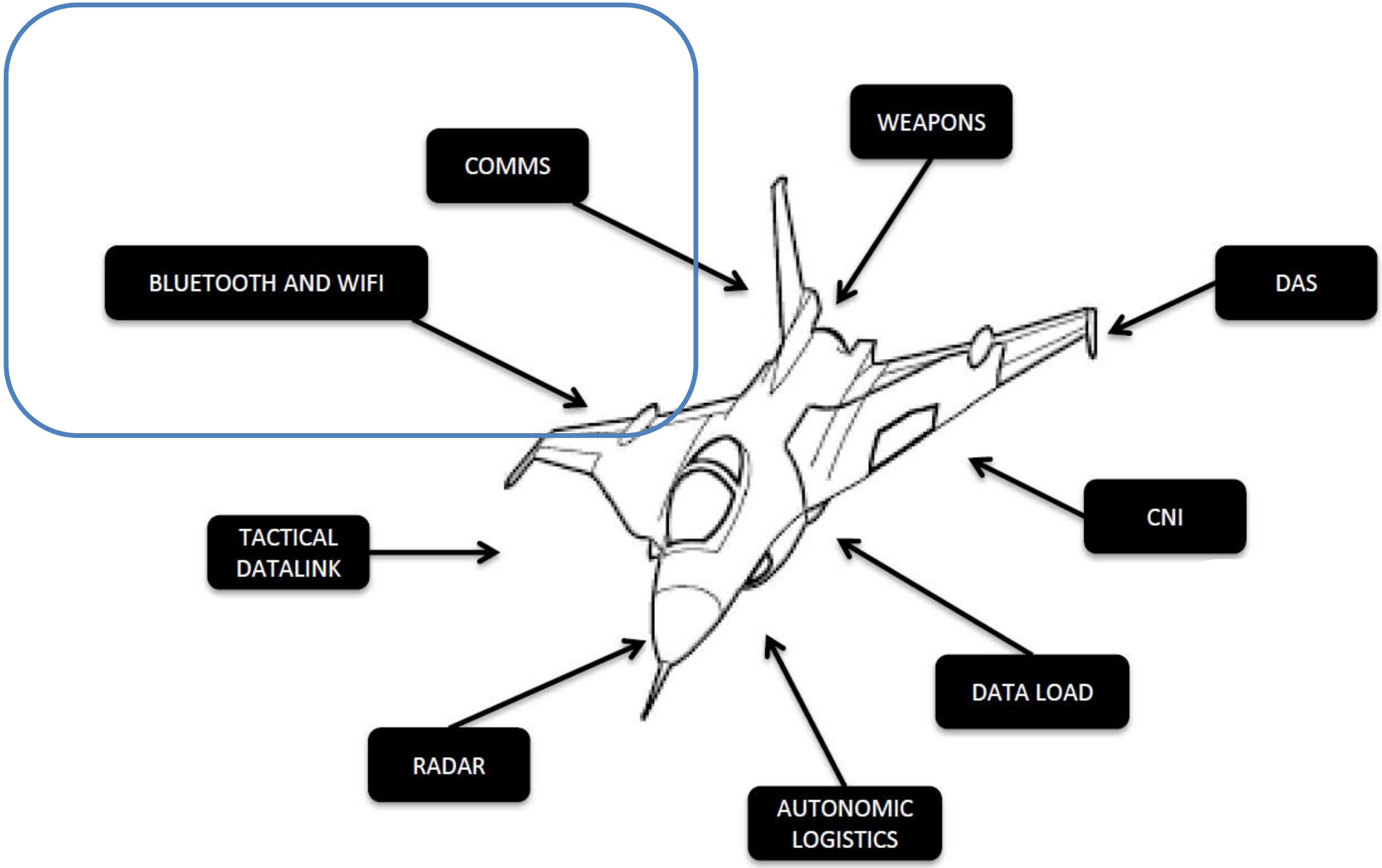




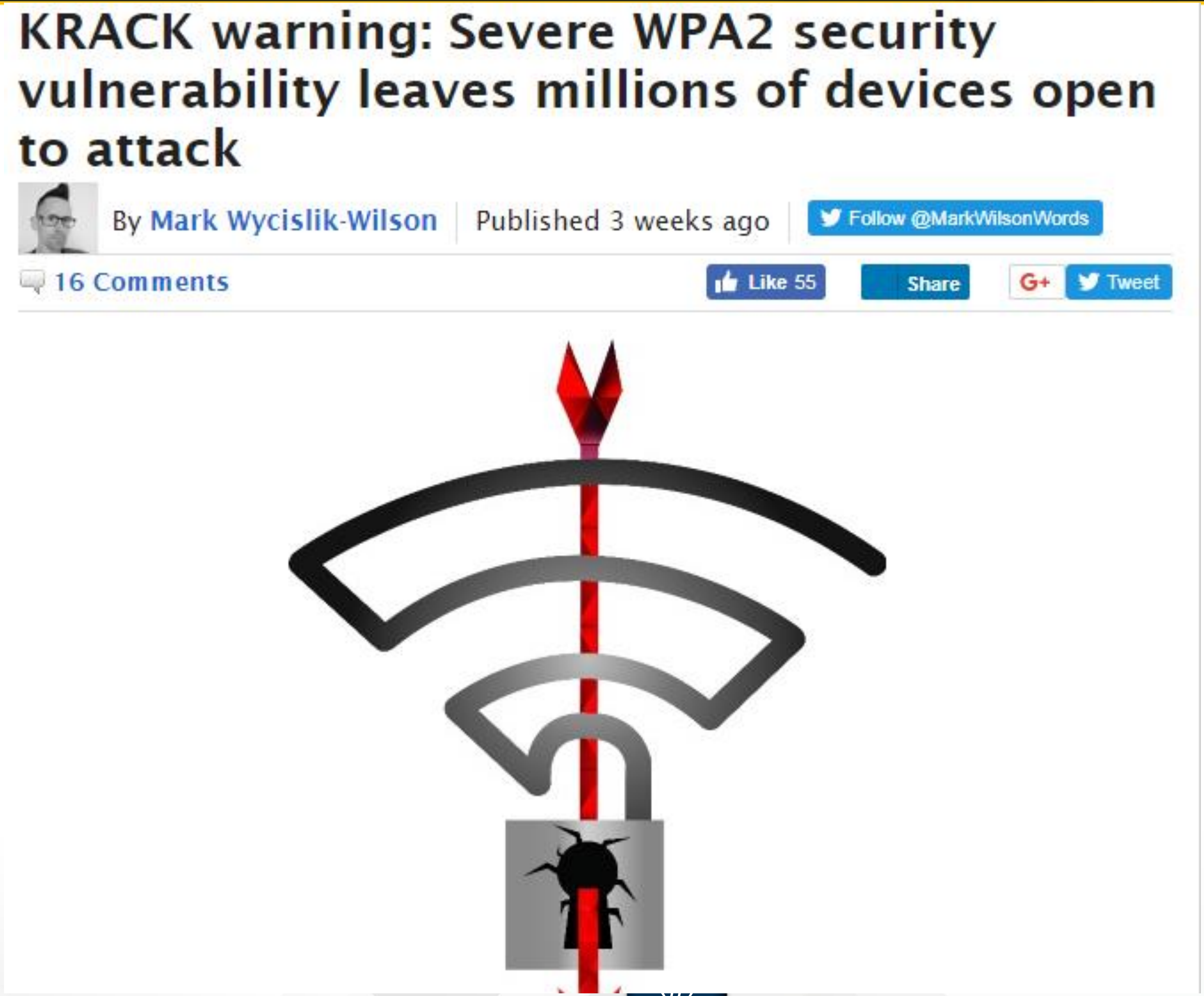

RESEARCHER SHOWS HOW TO HACK
(AND CRASH) A PASSENGER AIRCRAFT
WITH AN ANDROID PHONE...

https://www.forbes.com/sites/forbestechcouncil/2017/01/17/why-cybersecurity-should-be-the-biggest-concern-of-2017/#4890789c5218

The evolving aircraft…



What is not Vulnerable?

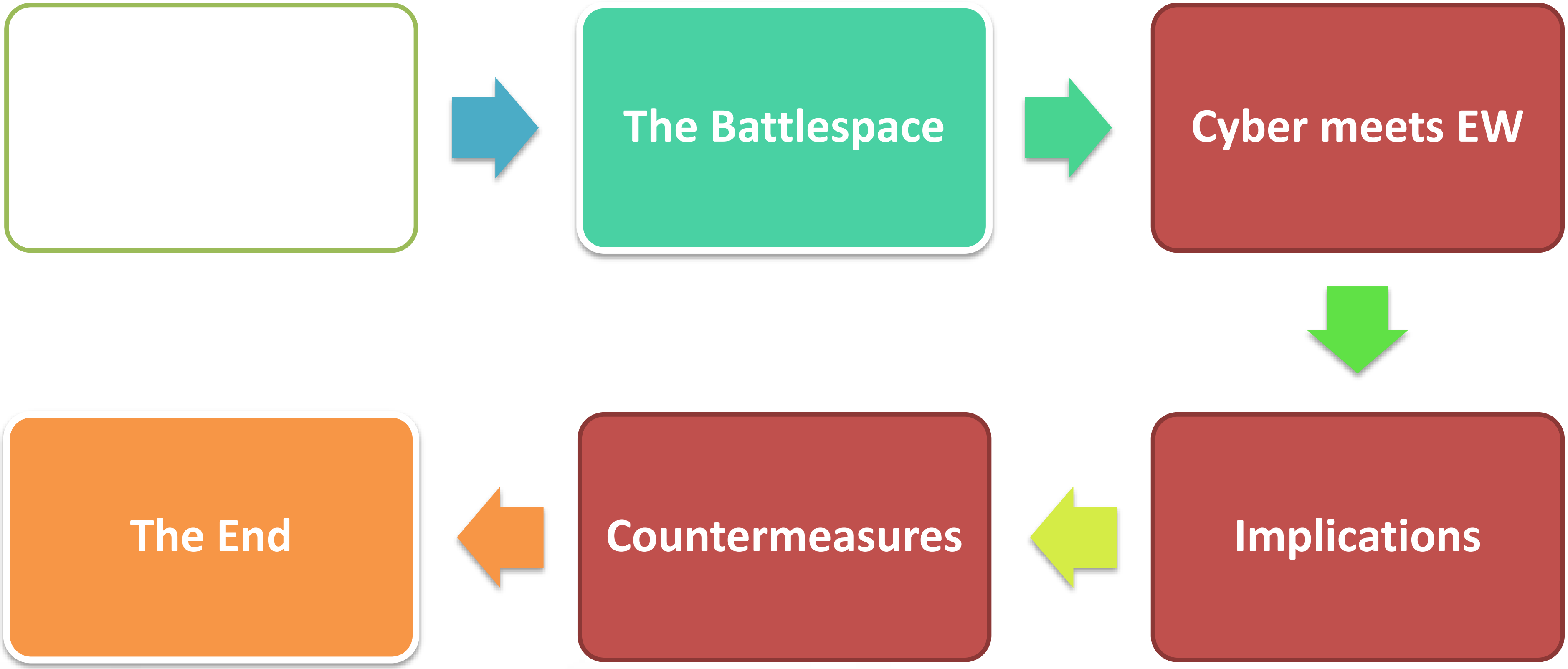


KRACK warning: Severe WPA2 security vulnerability leaves millions of devices open to attack

By Mark Wycislik-Wilson | Published 3 weeks ago

16 Comments

Progress…



The Battlespace

Cyber meets EW

Implications

Countermeasures

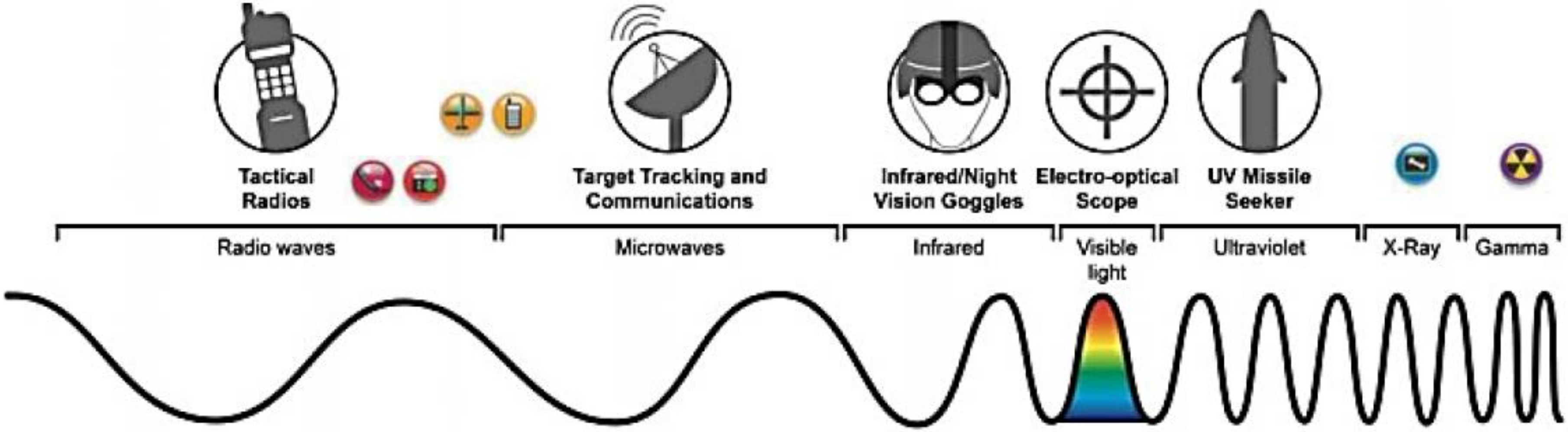
The End

Man-Made Cyber Space

GREENLAND
CANADA
RUSSIA
UNITED STATES
CHINA
MEXICO
INDIA
BRAZIL
AUSTRALIA
ARGENTINA

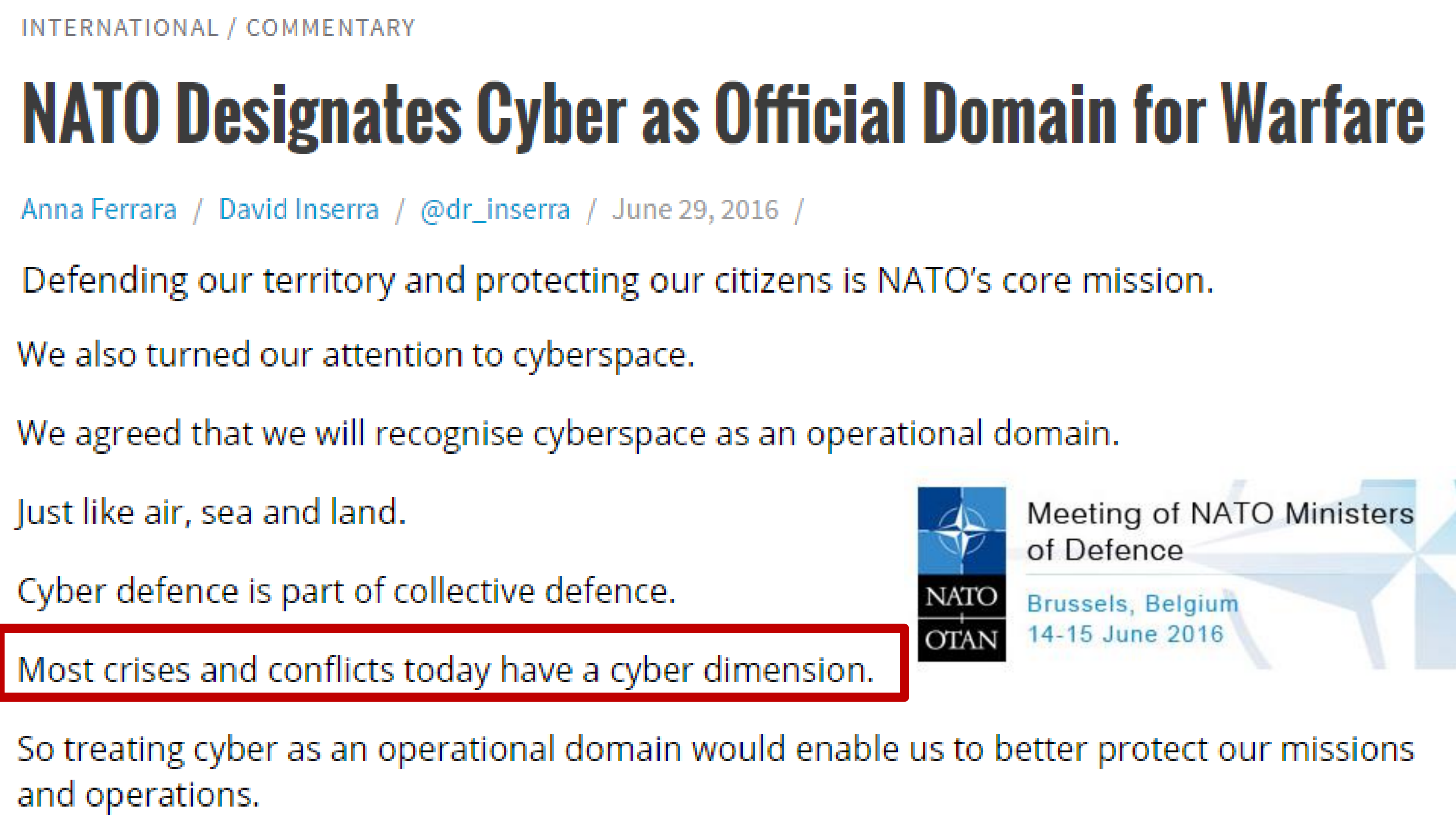
Source: Kaspersky lab

EM Space



The spectrum is becoming complex and with cyberspace, a war could be lost due to ignorance.

The Cyber Battlefield…



INTERNATIONAL / COMMENTARY

NATO Designates Cyber as Official Domain for Warfare

Anna Ferrara / David Inserra / @dr_inserra / June 29, 2016 /

Defending our territory and protecting our citizens is NATO's core mission.

We also turned our attention to cyberspace.

We agreed that we will recognise cyberspace as an operational domain.

Just like air, sea and land.

Cyber defence is part of collective defence.

Most crises and conflicts today have a cyber dimension.

So treating cyber as an operational domain would enable us to better protect our missions and operations.

Meeting of NATO Ministers of Defence

Brussels, Belgium
14-15 June 2016

About War…

State on State war using mass, objective and manoeuvre

Kinetic war for political objectives

Act of force to compel the enemy to do our will

Intelligence, Deception

Attack the mind of your enemies

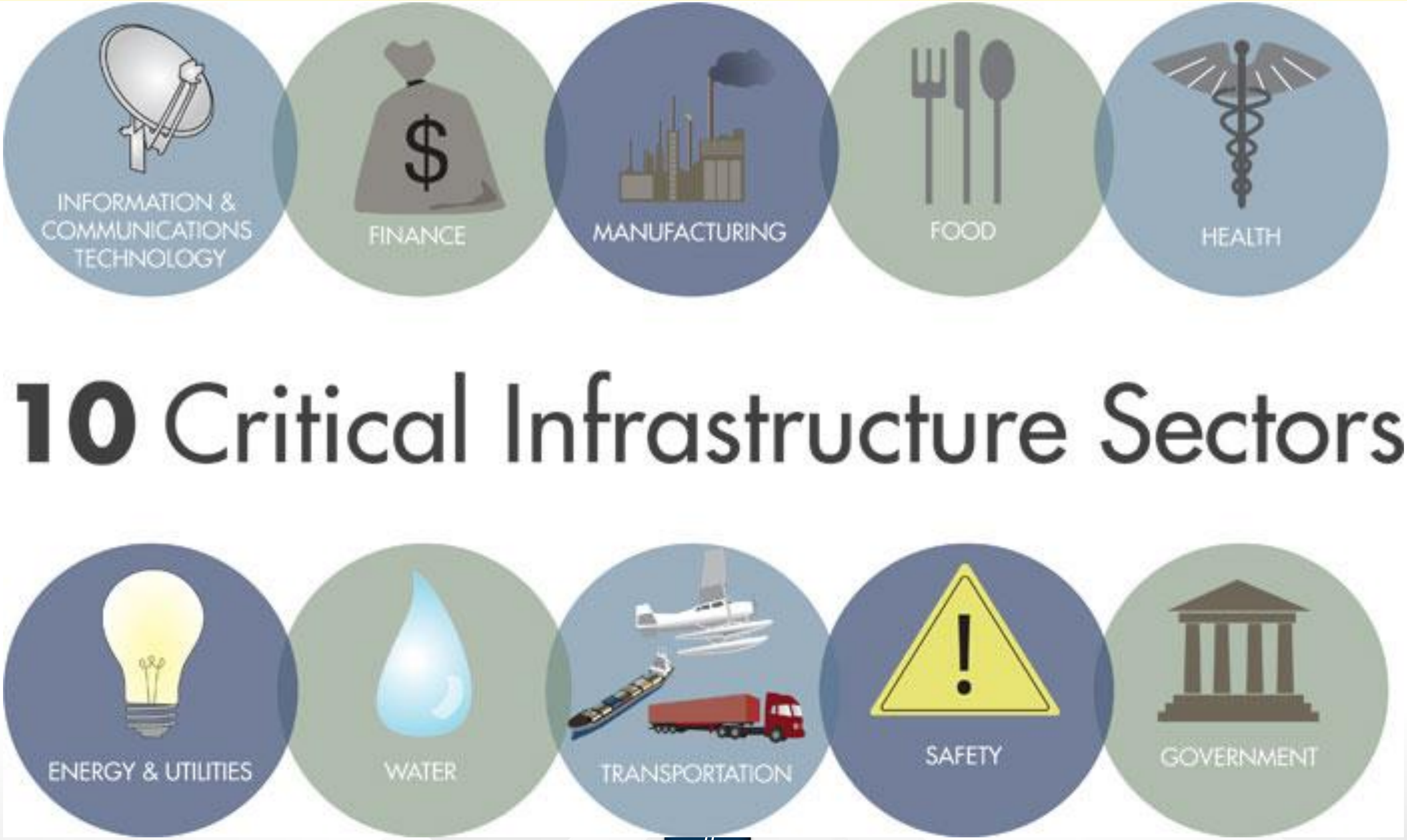
Subdue the enemy without fighting

"Observe, orient, decide and act more inconspicuously, more quickly, and with more irregularity …"

Boyd, Patterns of War

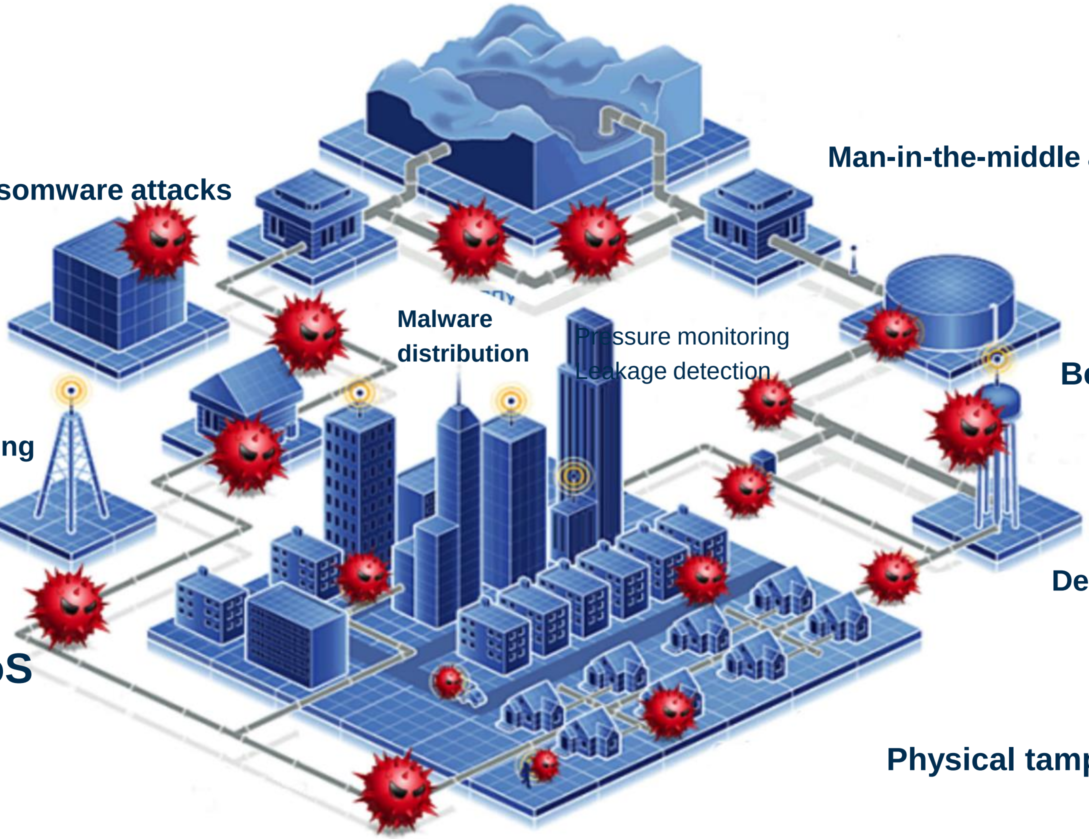
Developed from 'Principles of War for Cyberspace' Lt Col Steven E. Cahinin US Air War College 2011 *www.au.af.mil/au/afri/aspj/digital/pdf/articles/Jan-Feb.../Research-Cahanin.pdf*

Cyber-Physical Systems



http://www.iprem.ca/initiatives/InitiativesPics/CriticalInfrastructureSectors.jpg

Smart Grid – What could go wrong?



Ransomware attacks

Man-in-the-middle attack

Malware distribution

Pressure monitoring
Leakage detection

Behaviour alteration

Data transmission monitoring

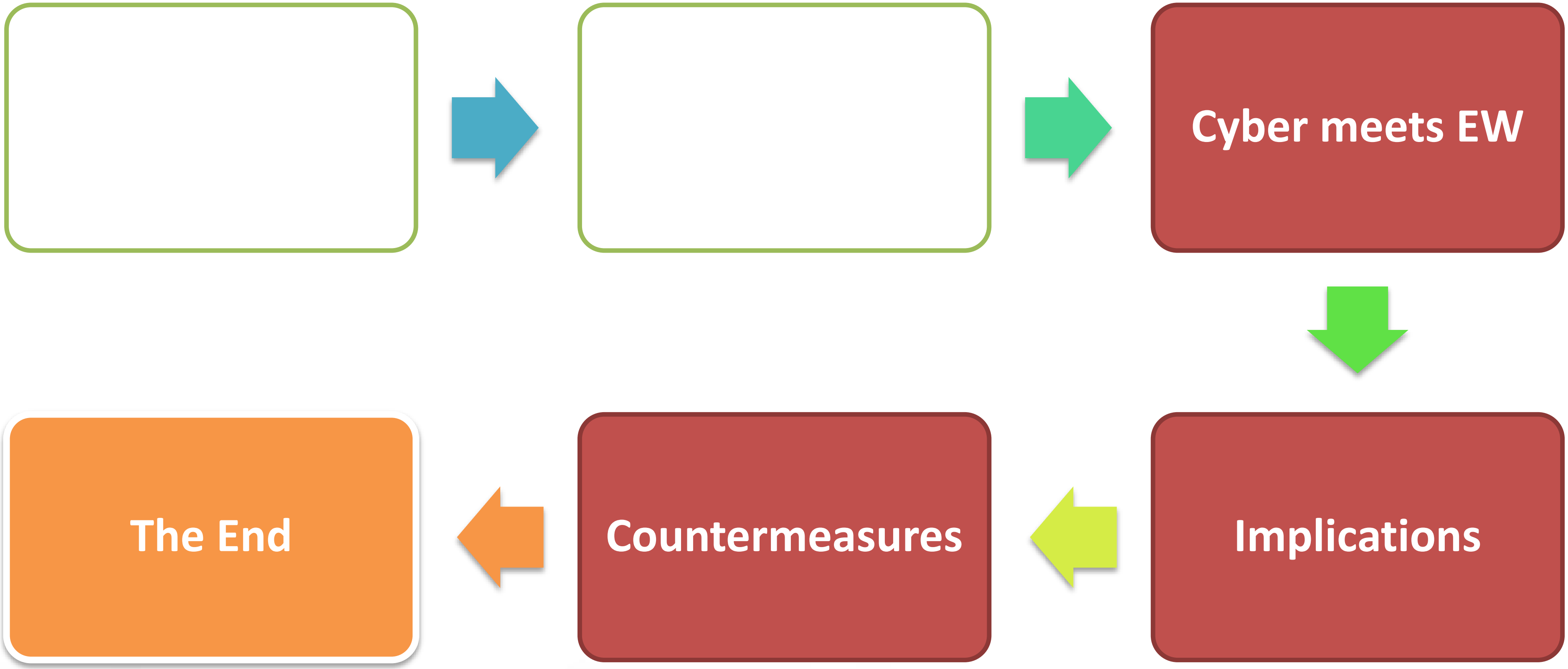
Deception attacks

DDoS

Physical tampering

Smart metering

Progress…



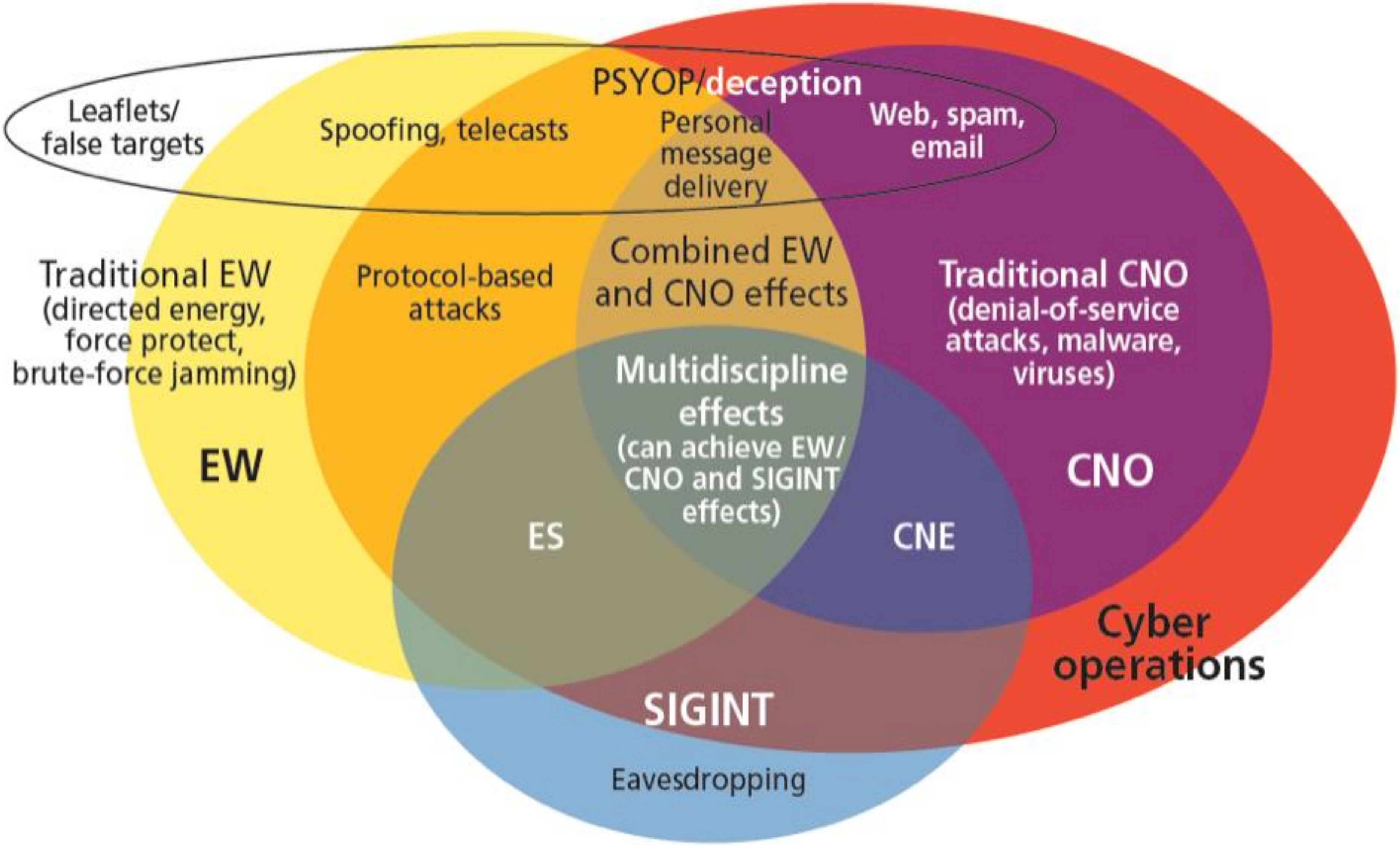
Cyber meets EW

Implications

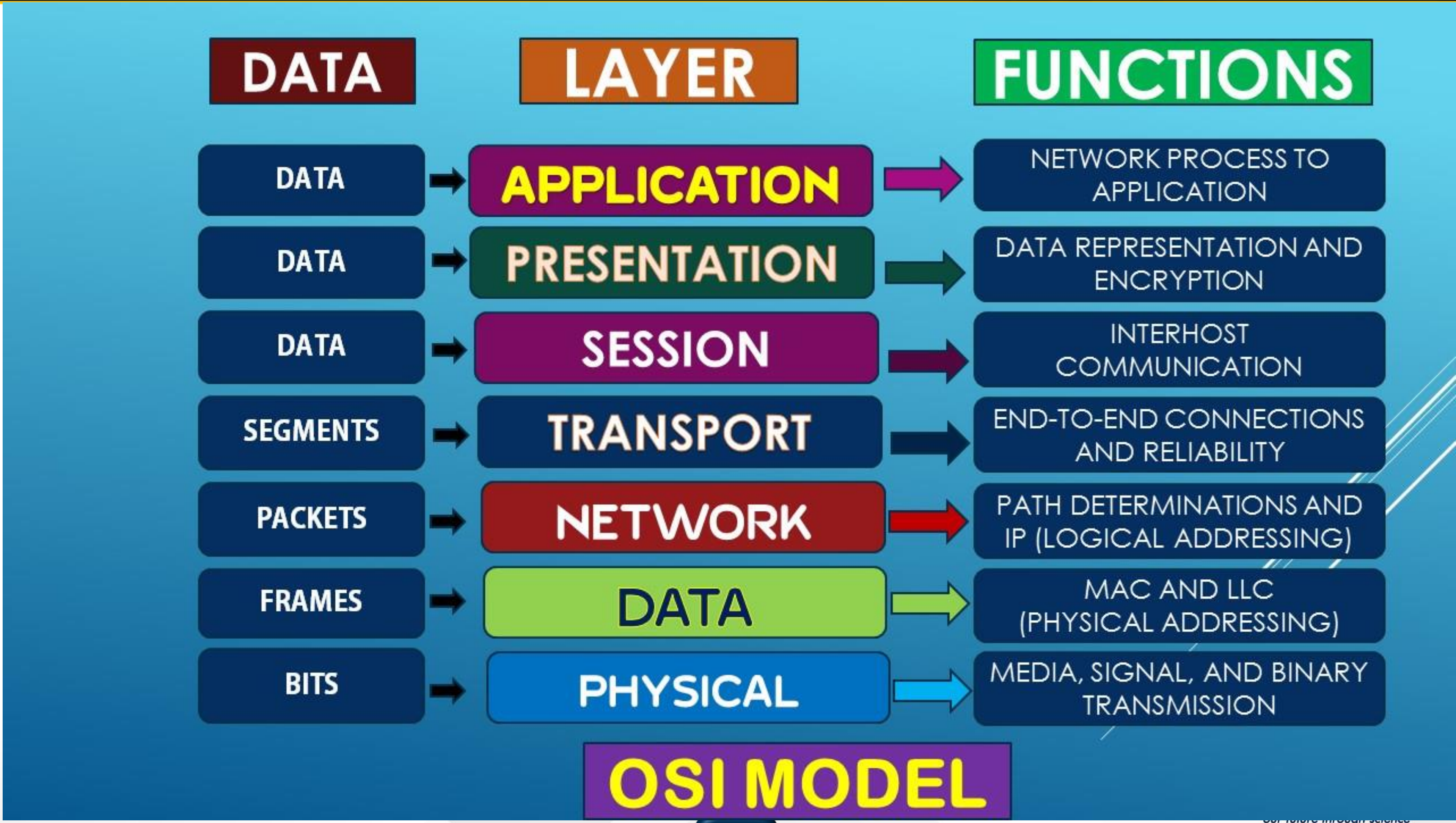
Countermeasures

The End

The Era of Convergence


PSYOP/deception
Leaflets/ false targets
Spoofing, telecasts
Personal message delivery
Web, spam, email
Traditional EW (directed energy, force protect, brute-force jamming)
Protocol-based attacks
Combined EW and CNO effects
Traditional CNO (denial-of-service attacks, malware, viruses)
Multidiscipline effects (can achieve EW/ CNO and SIGINT effects)
EW
CNO
ES
CNE
Cyber operations
SIGINT
Eavesdropping

Mapped by the OSI model



DATA	LAYER	FUNCTIONS
DATA	APPLICATION	NETWORK PROCESS TO APPLICATION
DATA	PRESENTATION	DATA REPRESENTATION AND ENCRYPTION
DATA	SESSION	INTERHOST COMMUNICATION
SEGMENTS	TRANSPORT	END-TO-END CONNECTIONS AND RELIABILITY
PACKETS	NETWORK	PATH DETERMINATIONS AND IP (LOGICAL ADDRESSING)
FRAMES	DATA	MAC AND LLC (PHYSICAL ADDRESSING)
BITS	PHYSICAL	MEDIA, SIGNAL, AND BINARY TRANSMISSION

OSI MODEL

Cyber & EW Similarities

Deny

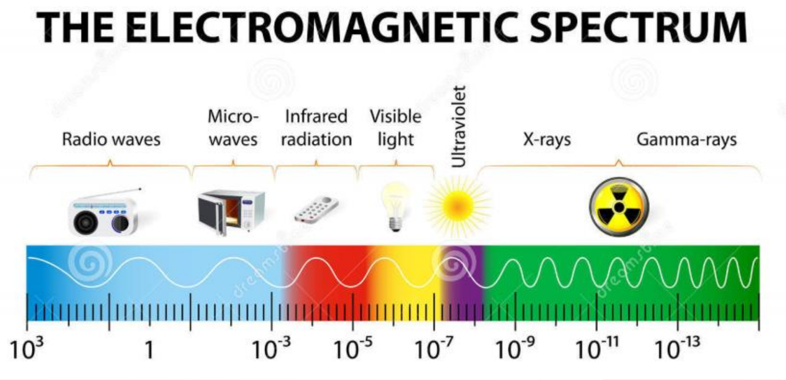
Disrupt

Deceive

Degrade

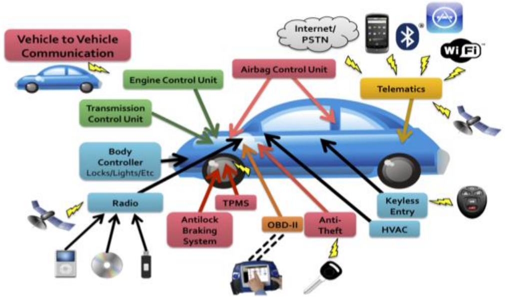
Destroy

Computers and Networks



Cyber-EW Convergence Opportunities

Maximum Effect



Diverse Attack Surface

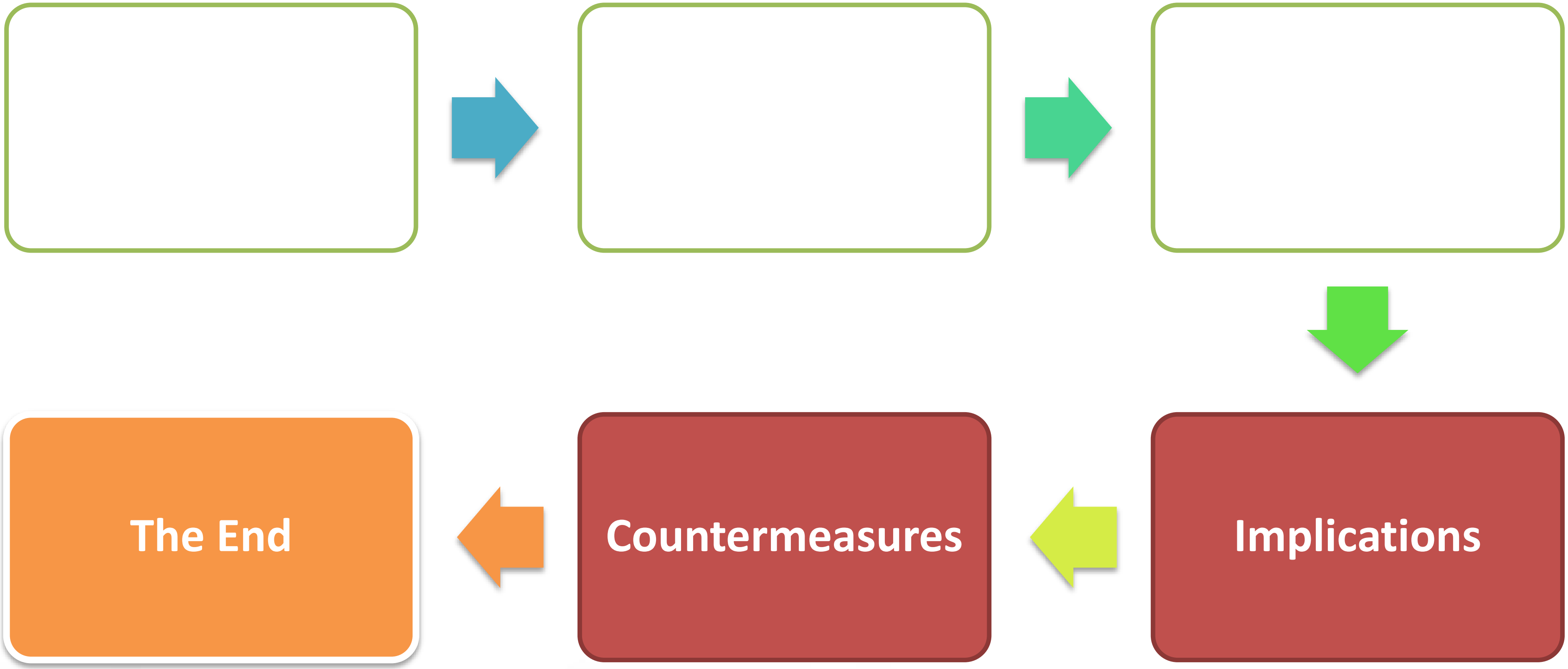
Deception & Weaponization

Zero-Seconds

Advance Persistent Threat

Advance Kill Chain

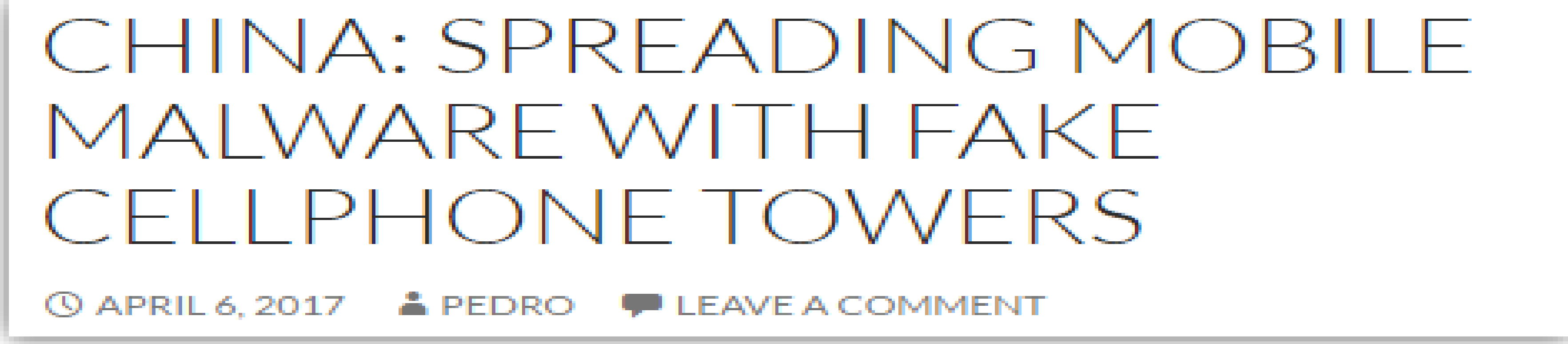
Progress…



Offense and Defense

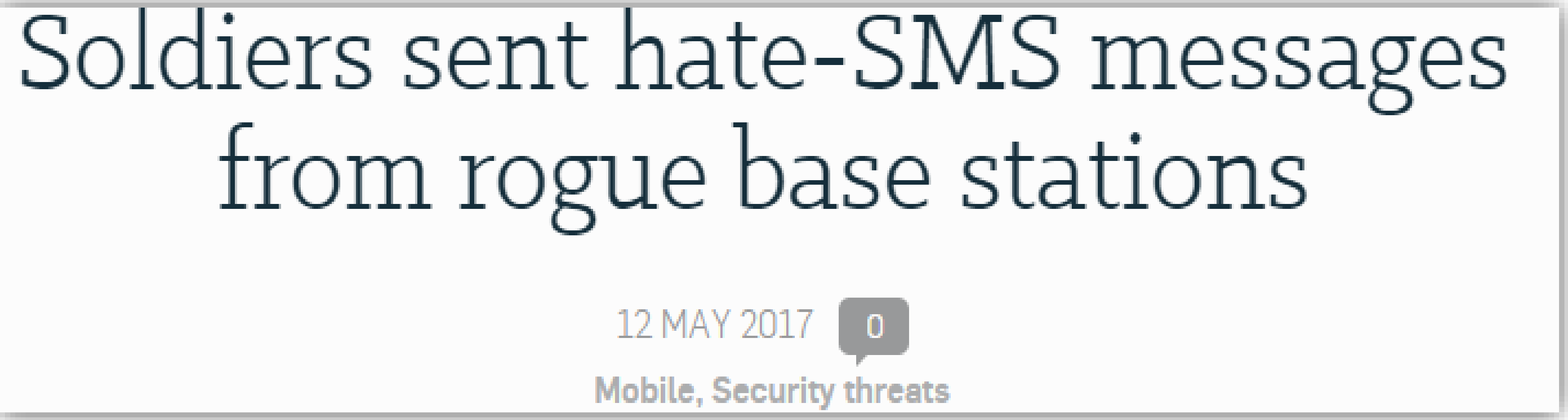
“When you think about attacking someone’s network, keep in mind that they can do the same to you…”

Case Studies: Cyber-EW Capabilities



CHINA: SPREADING MOBILE MALWARE WITH FAKE CELLPHONE TOWERS

APRIL 6, 2017 PEDRO LEAVE A COMMENT

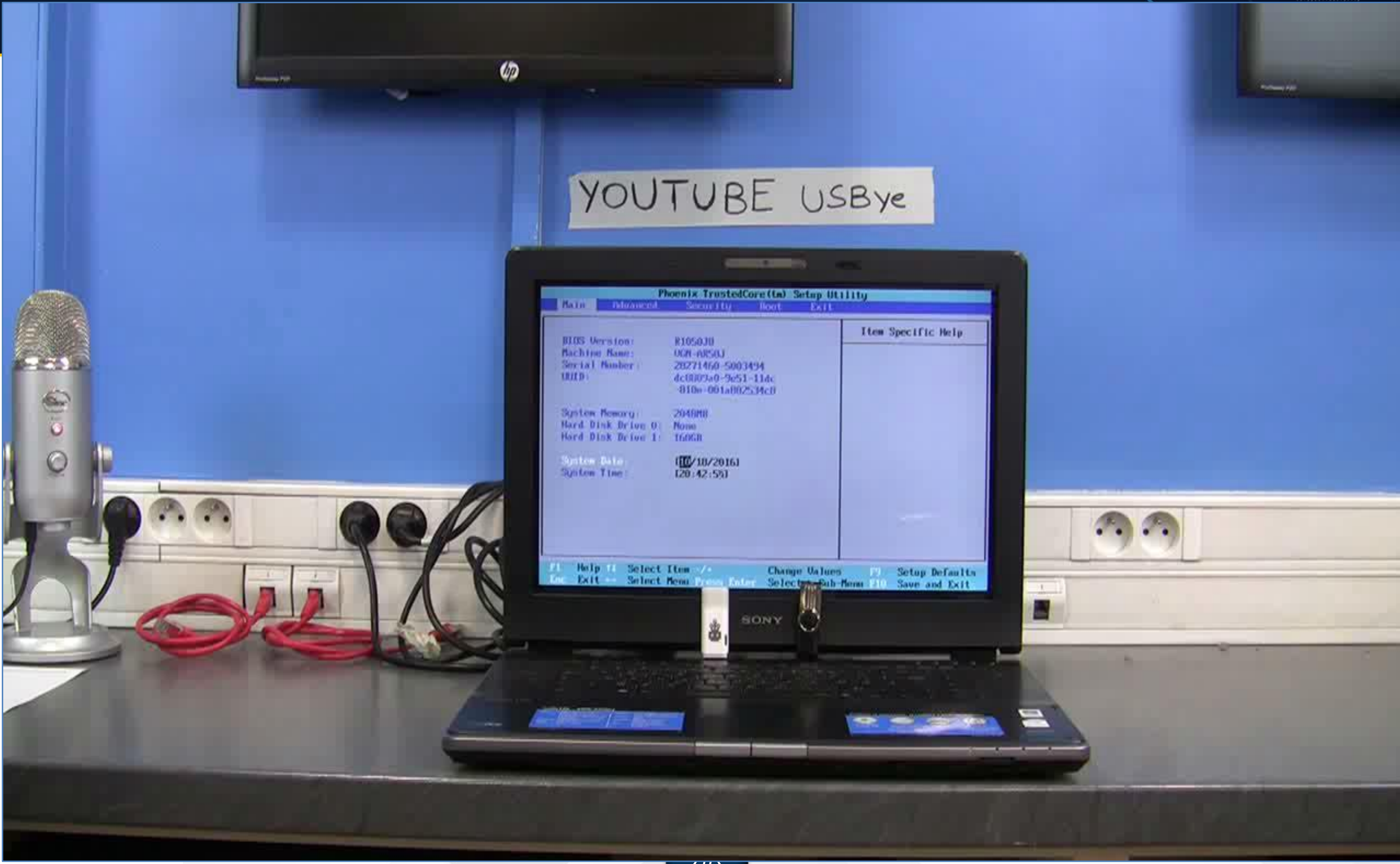


Soldiers sent hate-SMS messages from rogue base stations

12 MAY 2017 0

Mobile, Security threats

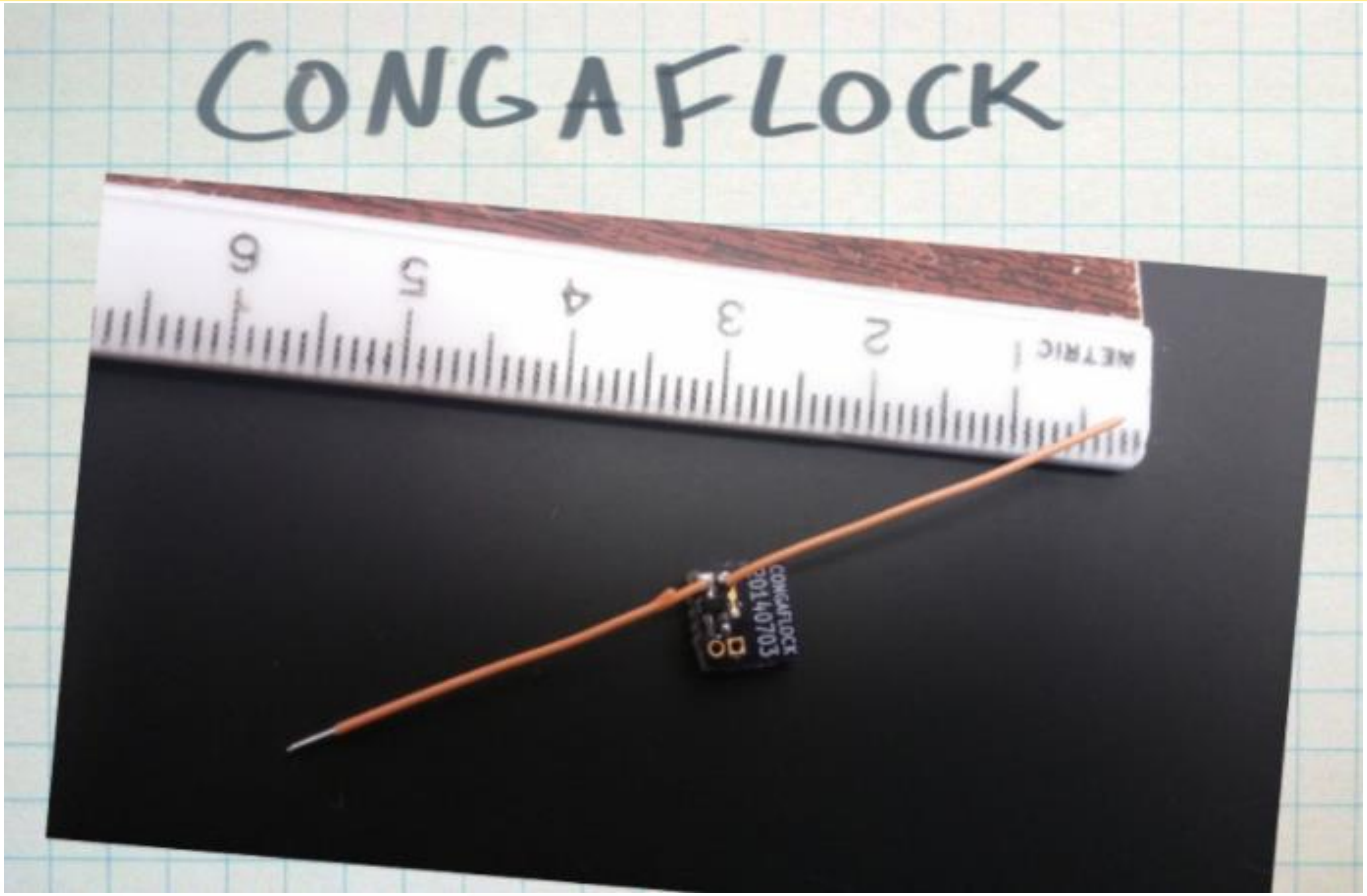
USB Killer


YOUTUBE USBye
Phoenix TrustedCore(tm) Setup Utility
Main Advanced Security Boot Exit
Item Specific Help
BIOS Version:
Machine Name:
Serial Number:
UUID:
System Memory: 2048MB
Hard Disk Drive 0: None
Hard Disk Drive 1: 160GB
System Date: [10/18/2016]
System Time: [20:42:58]
F1 Help Select Item Change Values F9 Setup Defaults
Esc Exit Select Menu Press Enter Select Sub-Menu F10 Save and Exit
SONY

NSA Playset

NSA Playset

NSA Playset



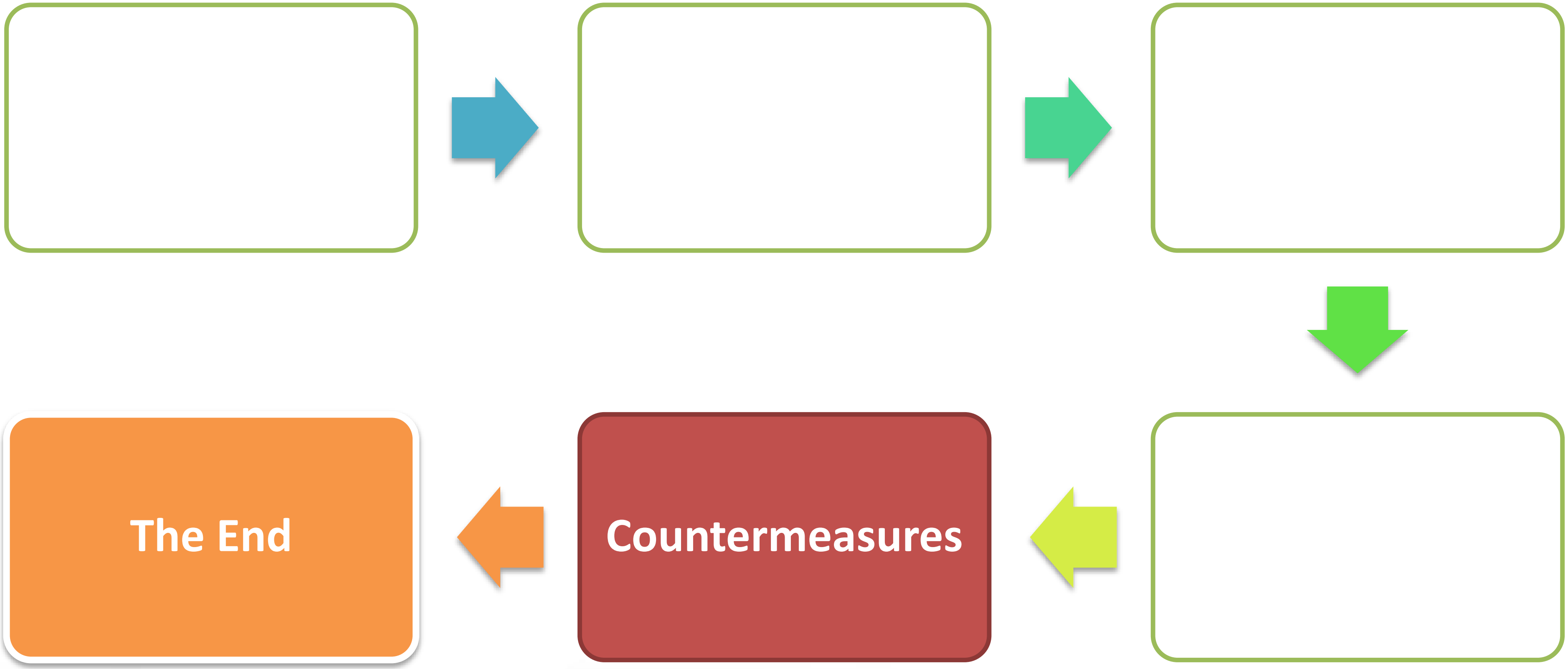
Some thought…

IDEAS THAT WORK FOR
INDUSTRIAL
DEVELOPMENT

“A modern thief can steal more with a computer than with a gun, cause more damage with a keyboard than a bomb.”

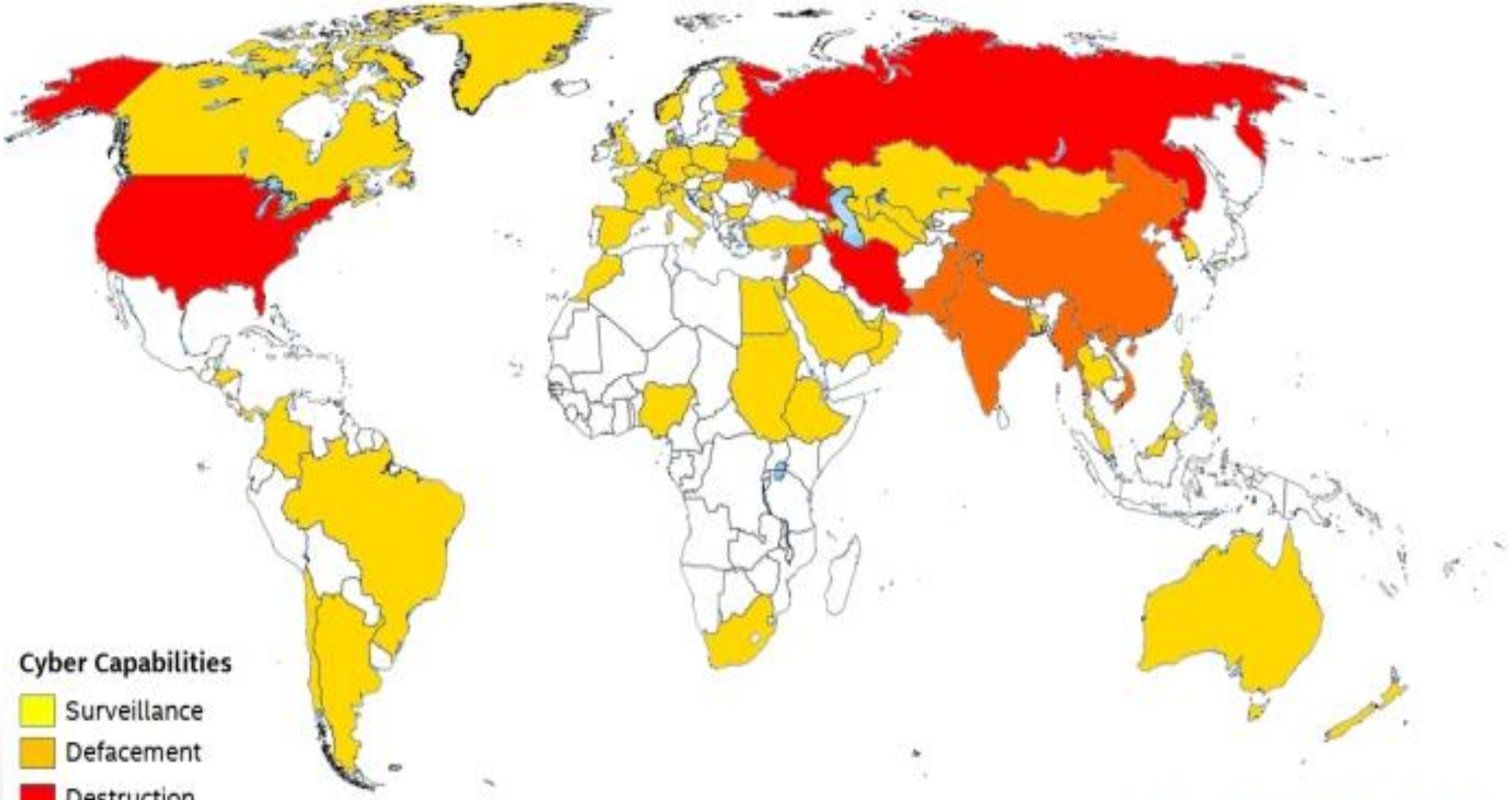
CSIR
our future through science

Progress…



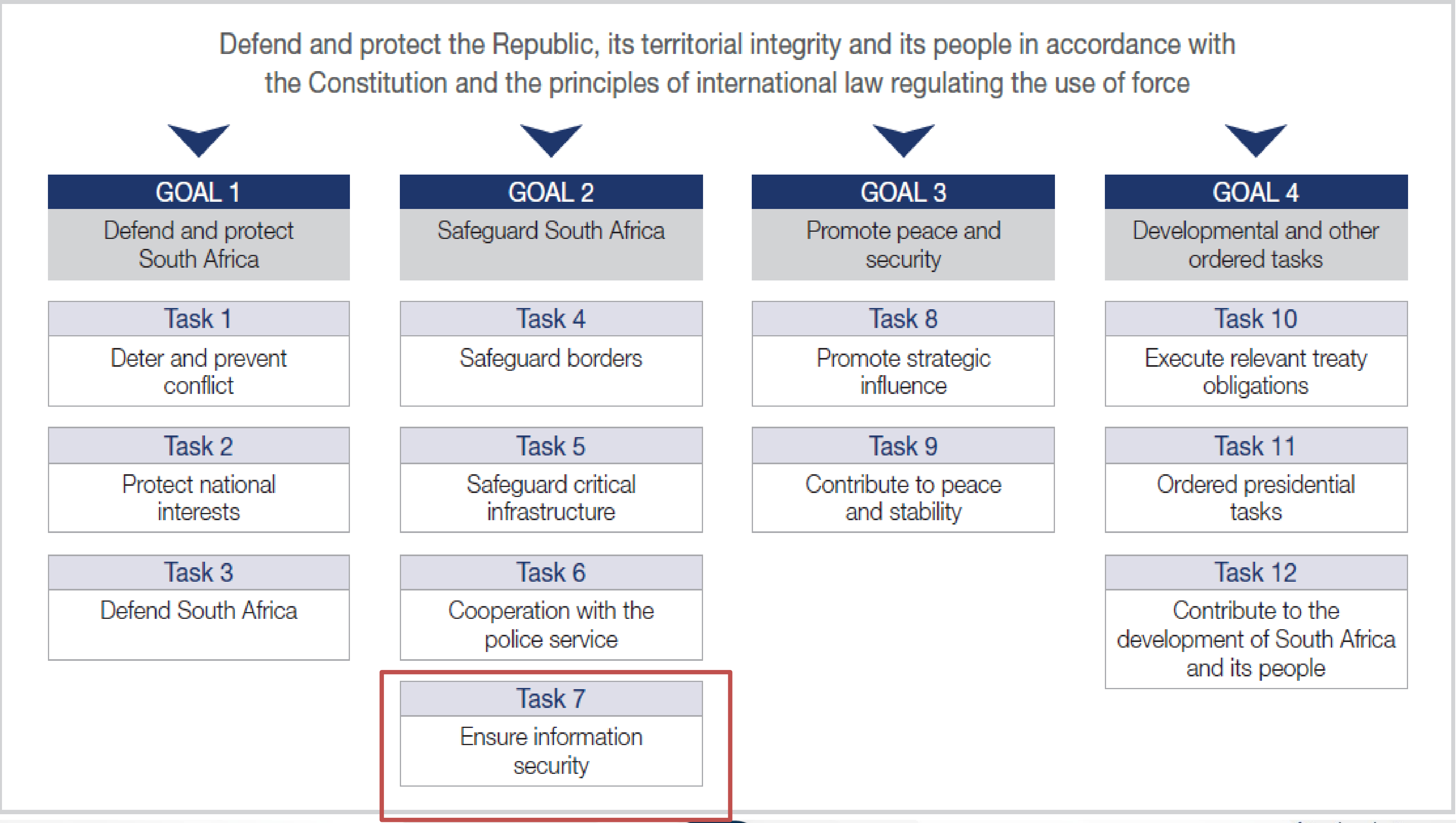
Preparation meets Opportunity

World's Cyberforces 2015



Data Source: Wall Street Journal – Cataloging the World's Cyberforces

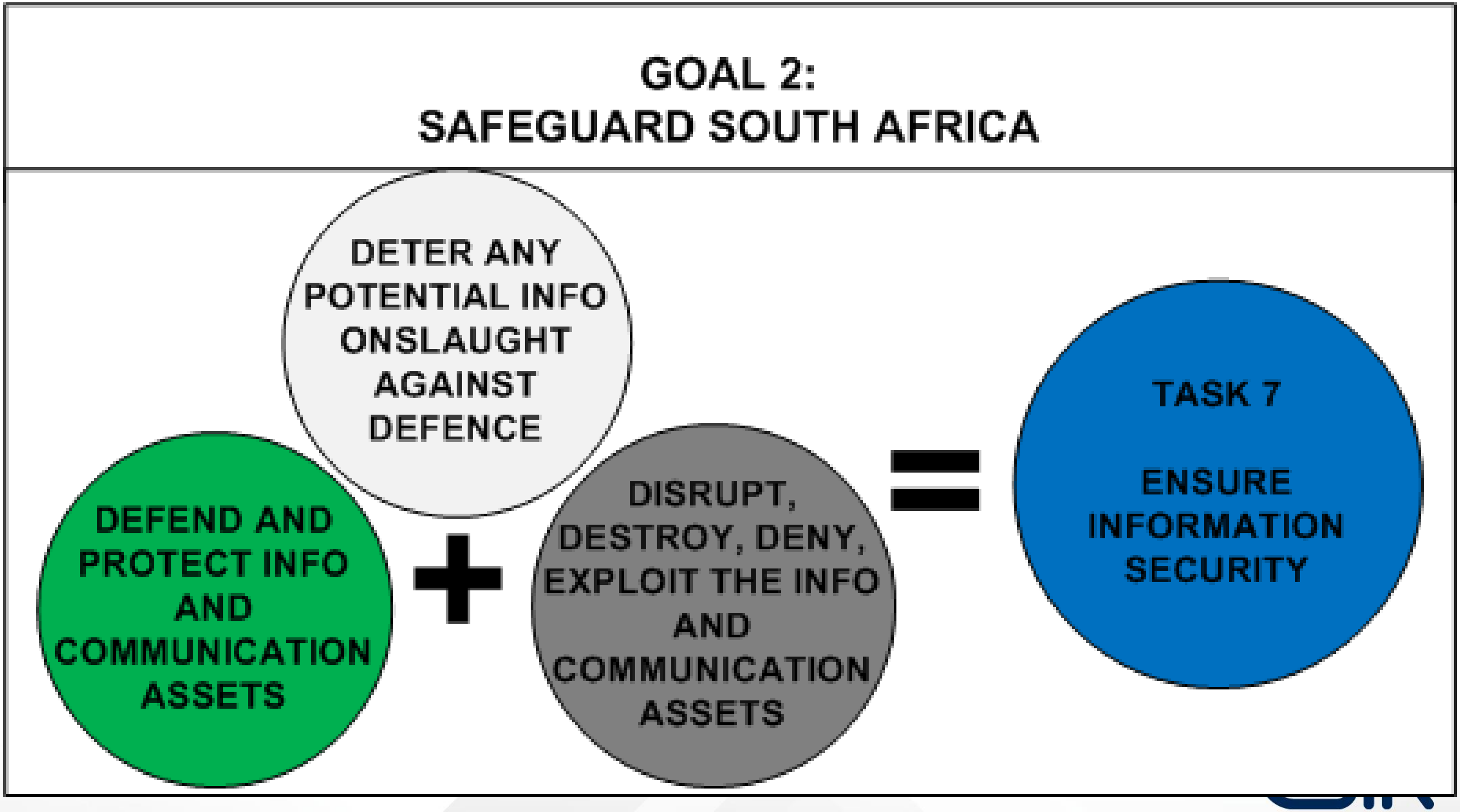
Defense Review



Defend and protect the Republic, its territorial integrity and its people in accordance with the Constitution and the principles of international law regulating the use of force

GOAL 1	GOAL 2	GOAL 3	GOAL 4
Defend and protect South Africa	Safeguard South Africa	Promote peace and security	Developmental and other ordered tasks
Task 1 Deter and prevent conflict	Task 4 Safeguard borders	Task 8 Promote strategic influence	Task 10 Execute relevant treaty obligations
Task 2 Protect national interests	Task 5 Safeguard critical infrastructure	Task 9 Contribute to peace and stability	Task 11 Ordered presidential tasks
Task 3 Defend South Africa	Task 6 Cooperation with the police service		Task 12 Contribute to the development of South Africa and its people
	Task 7 Ensure information security		

Defensive & Offensive Capabilities



GOAL 2:
SAFEGUARD SOUTH AFRICA

DEFEND AND PROTECT INFO AND COMMUNICATION ASSETS

+

DETER ANY POTENTIAL INFO ONSLAUGHT AGAINST DEFENCE

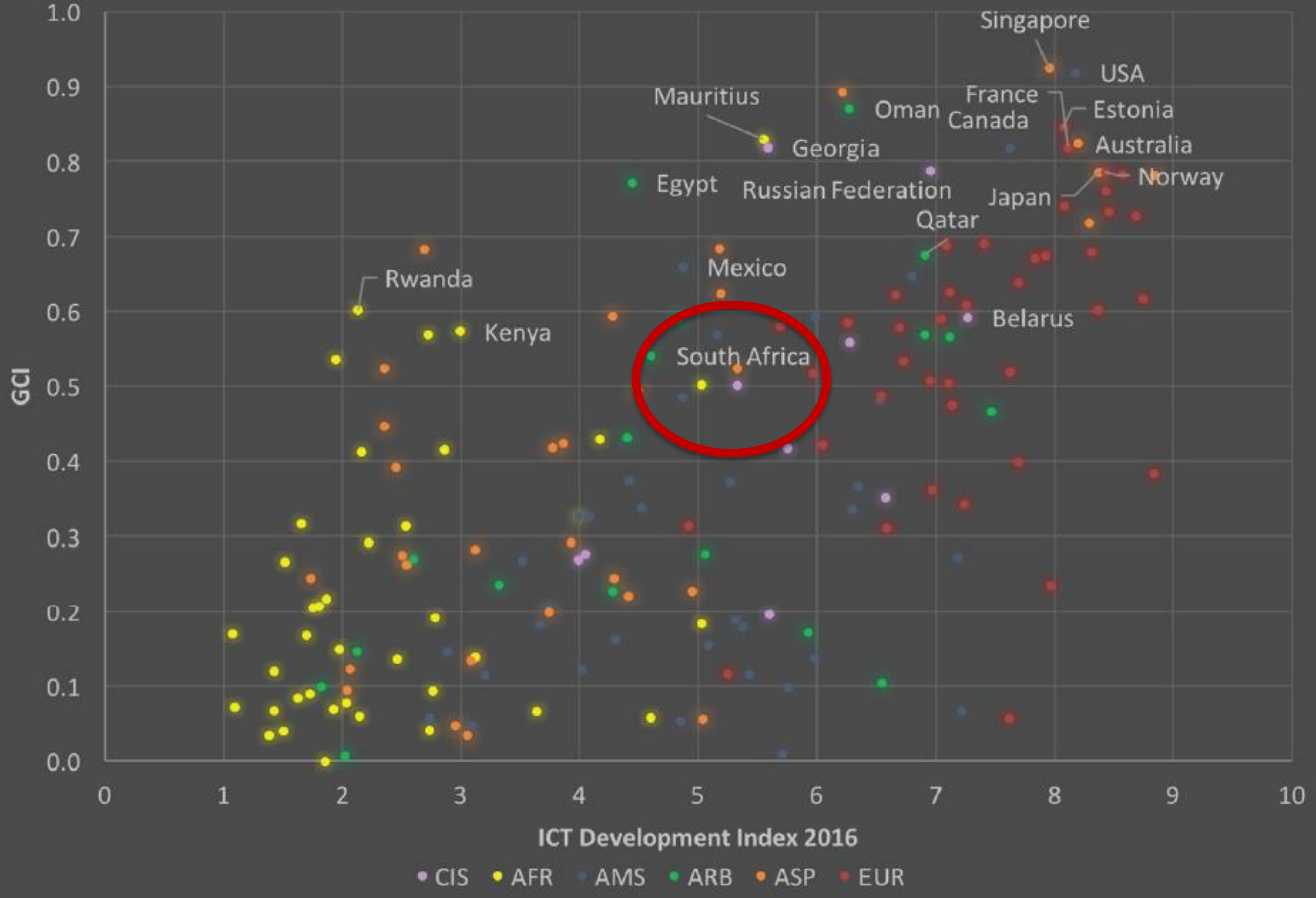
DISRUPT, DESTROY, DENY, EXPLOIT THE INFO AND COMMUNICATION ASSETS

=

TASK 7

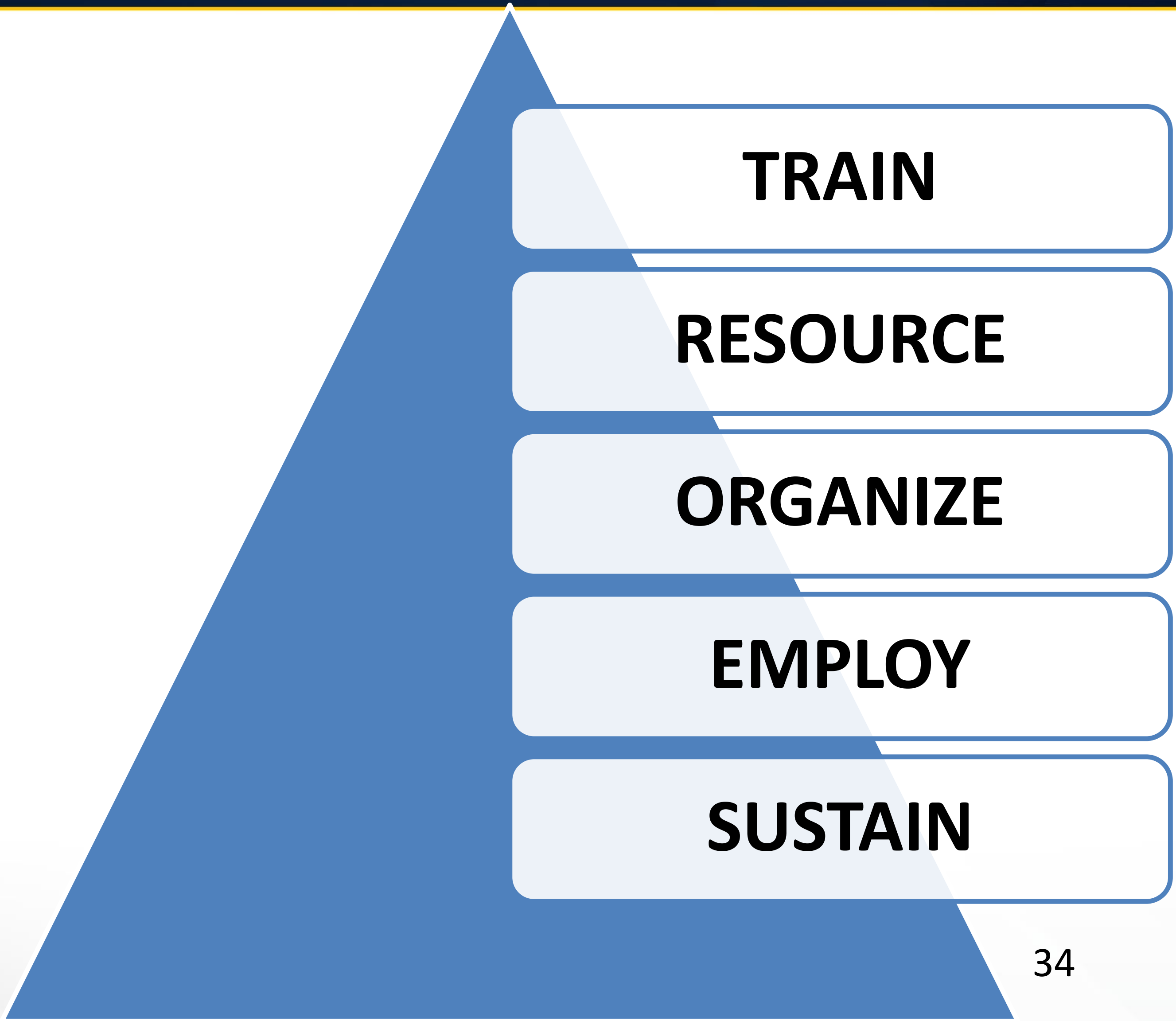
ENSURE INFORMATION SECURITY

GCI - IDI 2016

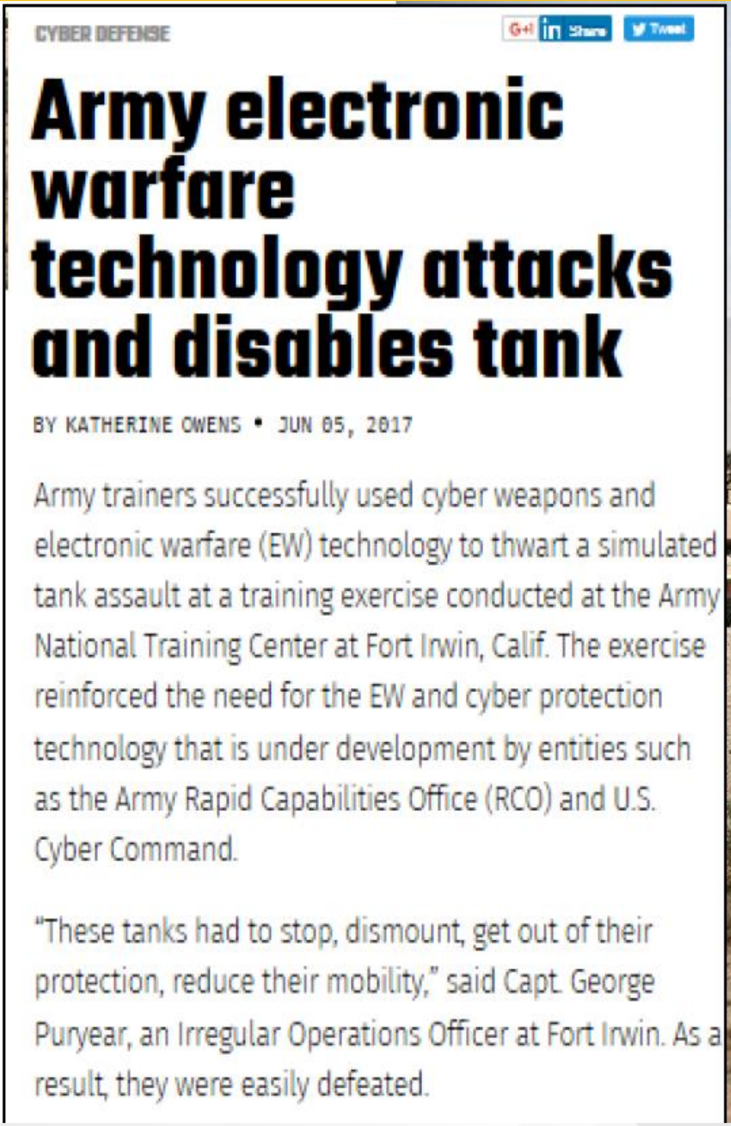


GCI
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
0
1
2
3
4
5
6
7
8
9
10
ICT Development Index 2016
Singapore
USA
France
Estonia
Oman
Canada
Australia
Mauritius
Georgia
Norway
Egypt
Russian Federation
Japan
Qatar
Mexico
Rwanda
Belarus
Kenya
South Africa
● CIS
● AFR
● AMS
● ARB
● ASP
● EUR

What can we do?



The train is moving…


G+
in Share
Tweet

CYBER DEFENSE

Army electronic warfare technology attacks and disables tank

BY KATHERINE OWENS • JUN 05, 2017

Army trainers successfully used cyber weapons and electronic warfare (EW) technology to thwart a simulated tank assault at a training exercise conducted at the Army National Training Center at Fort Irwin, Calif. The exercise reinforced the need for the EW and cyber protection technology that is under development by entities such as the Army Rapid Capabilities Office (RCO) and U.S. Cyber Command.

"These tanks had to stop, dismount, get out of their protection, reduce their mobility," said Capt. George Puryear, an Irregular Operations Officer at Fort Irwin. As a result, they were easily defeated.

DEFENSE SYSTEMS

Adapt or Perish…

"We must learn to negotiate the new Geography where borders are irrelevant, distance meaningless…enemy can harm our vital systems without confronting our strongest force."

Protection of Critical Infrastructure Commission (1997)

IDEAS THAT WORK FOR
INDUSTRIAL
DEVELOPMENT

Thank You

jmtsweni@csir.co.za

CSIR
our future through science