Perspectives on Cyber Operations

BG (AF) Francesco VESTITO
JOCC Commander

Rome, 25th March 2019

SITUATION

SPACENEWS

NEWS | OPINION | VIDEO | LAUNCH | BUSINESS

Growing U.S. satellite vulnerability: The silent 'Apocalypse Next'

by Brian G. Chow ar

DoDBUZZ

› News › DoDBuzz

The Telegra

News

UK | World | I

US, Coalition Forces Used Cyberattacks to Hunt Down ISIS Command Posts

› News

British Airways hacking: Customers cancel credit cards as airline defends handling of 'sophisticated' cyber attack

PRESIDENZA DELLA REPUBBLICA

Cerca

Home › archivio › discorso

Pres. Mattarella: "cyberspace truly is a place of freedom and not a place of hostility and danger"

Security | Social Networks | Terrorism | EXTENDED CO

Many misconfigured Tor sites expose the public IP address via SSL certificates

The Telegraph

HOME | NEWS | S

News

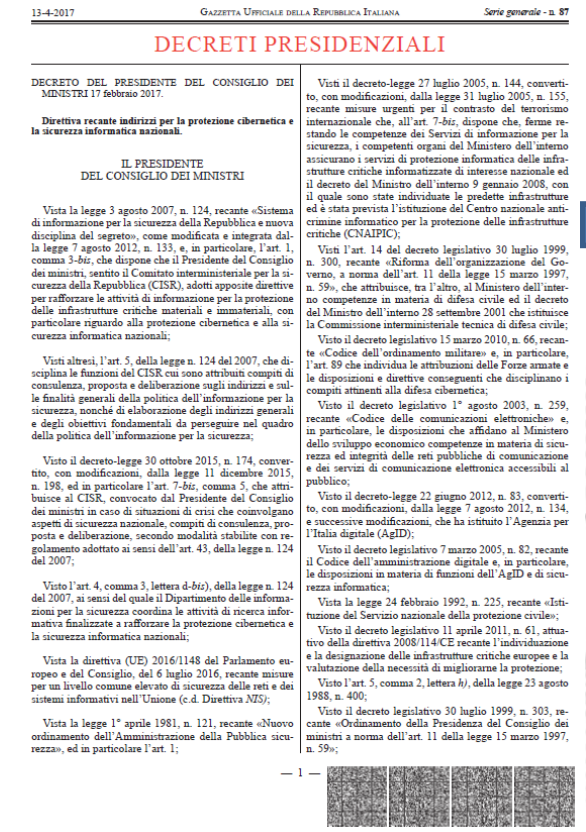
UK | World | Politics | Science | Education | Health | Brexit | Royals | Investigatio

› News

Cyber attack on Singapore health database steals details of 1.5m including prime minister

NATIONAL CYBER FRAMEWORK

DPCM 17th Feb. 2017
National strategy for cyber security



13-4-2017 GAZZETTA UFFICIALE DELLA REPUBBLICA ITALIANA Serie generale - n. 87

DECRETI PRESIDENZIALI

DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 17 febbraio 2017.

Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali.

IL PRESIDENTE
DEL CONSIGLIO DEI MINISTRI

Vista la legge 3 agosto 2007, n. 124, recante «Sistema di informazione per la sicurezza della Repubblica e nuova disciplina del segreto», come modificata e integrata dalla legge 7 agosto 2012, n. 133, e, in particolare, l'art. 1, comma 3-*bis*, che dispone che il Presidente del Consiglio dei ministri, sentito il Comitato interministeriale per la sicurezza della Repubblica (CISR), adotti apposite direttive per rafforzare le attività di informazione per la protezione delle infrastrutture critiche materiali e immateriali, con particolare riguardo alla protezione cibernetica e alla sicurezza informatica nazionali;

Visti altresì, l'art. 5, della legge n. 124 del 2007, che disciplina le funzioni del CISR cui sono attribuiti compiti di consulenza, proposta e deliberazione sugli indirizzi e sulle finalità generali della politica dell'informazione per la sicurezza, nonché di elaborazione degli indirizzi generali e degli obiettivi fondamentali da perseguire nel quadro della politica dell'informazione per la sicurezza;

Visto il decreto-legge 30 ottobre 2015, n. 174, convertito, con modificazioni, dalla legge 11 dicembre 2015, n. 198, ed in particolare l'art. 7-*bis*, comma 5, che attribuisce al CISR, convocato dal Presidente del Consiglio dei ministri in caso di situazioni di crisi che coinvolgano aspetti di sicurezza nazionale, compiti di consulenza, proposta e deliberazione, secondo modalità stabilite con regolamento adottato ai sensi dell'art. 43, della legge n. 124 del 2007;

Visto l'art. 4, comma 3, lettera d-*bis*), della legge n. 124 del 2007, ai sensi del quale il Dipartimento delle informazioni per la sicurezza coordina le attività di ricerca informativa finalizzate a rafforzare la protezione cibernetica e la sicurezza informatica nazionali;

Vista la direttiva (UE) 2016/1148 del Parlamento europeo e del Consiglio, del 6 luglio 2016, recante misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione (c.d. Direttiva *NIS*);

Vista la legge 1° aprile 1981, n. 121, recante «Nuovo ordinamento dell'Amministrazione della Pubblica sicurezza», ed in particolare l'art. 1;

Visti il decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, recante misure urgenti per il contrasto del terrorismo internazionale che, all'art. 7-*bis*, dispone che, ferme restando le competenze dei Servizi di informazione per la sicurezza, i competenti organi del Ministero dell'interno assicurano i servizi di protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale ed il decreto del Ministro dell'interno 9 gennaio 2008, con il quale sono state individuate le predette infrastrutture ed è stata prevista l'istituzione del Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche (CNAIPIC);

Visti l'art. 14 del decreto legislativo 30 luglio 1999, n. 300, recante «Riforma dell'organizzazione del Governo, a norma dell'art. 11 della legge 15 marzo 1997, n. 59», che attribuisce, tra l'altro, al Ministero dell'interno competenze in materia di difesa civile ed il decreto del Ministro dell'interno 28 settembre 2001 che istituisce la Commissione interministeriale tecnica di difesa civile;

Visto il decreto legislativo 15 marzo 2010, n. 66, recante «Codice dell'ordinamento militare» e, in particolare, l'art. 89 che individua le attribuzioni delle Forze armate e le disposizioni e direttive conseguenti che disciplinano i compiti attinenti alla difesa cibernetica;

Visto il decreto legislativo 1° agosto 2003, n. 259, recante «Codice delle comunicazioni elettroniche» e, in particolare, le disposizioni che affidano al Ministero dello sviluppo economico competenze in materia di sicurezza ed integrità delle reti pubbliche di comunicazione e dei servizi di comunicazione elettronica accessibili al pubblico;

Visto il decreto-legge 22 giugno 2012, n. 83, convertito, con modificazioni, dalla legge 7 agosto 2012, n. 134, e successive modificazioni, che ha istituito l'Agenzia per l'Italia digitale (AgID);

Visto il decreto legislativo 7 marzo 2005, n. 82, recante il Codice dell'amministrazione digitale e, in particolare, le disposizioni in materia di funzioni dell'AgID e di sicurezza informatica;

Vista la legge 24 febbraio 1992, n. 225, recante «Istituzione del Servizio nazionale della protezione civile»;

Visto il decreto legislativo 11 aprile 2011, n. 61, attuativo della direttiva 2008/114/CE recante l'individuazione e la designazione delle infrastrutture critiche europee e la valutazione della necessità di migliorarne la protezione;

Visto l'art. 5, comma 2, lettera *b)*, della legge 23 agosto 1988, n. 400;

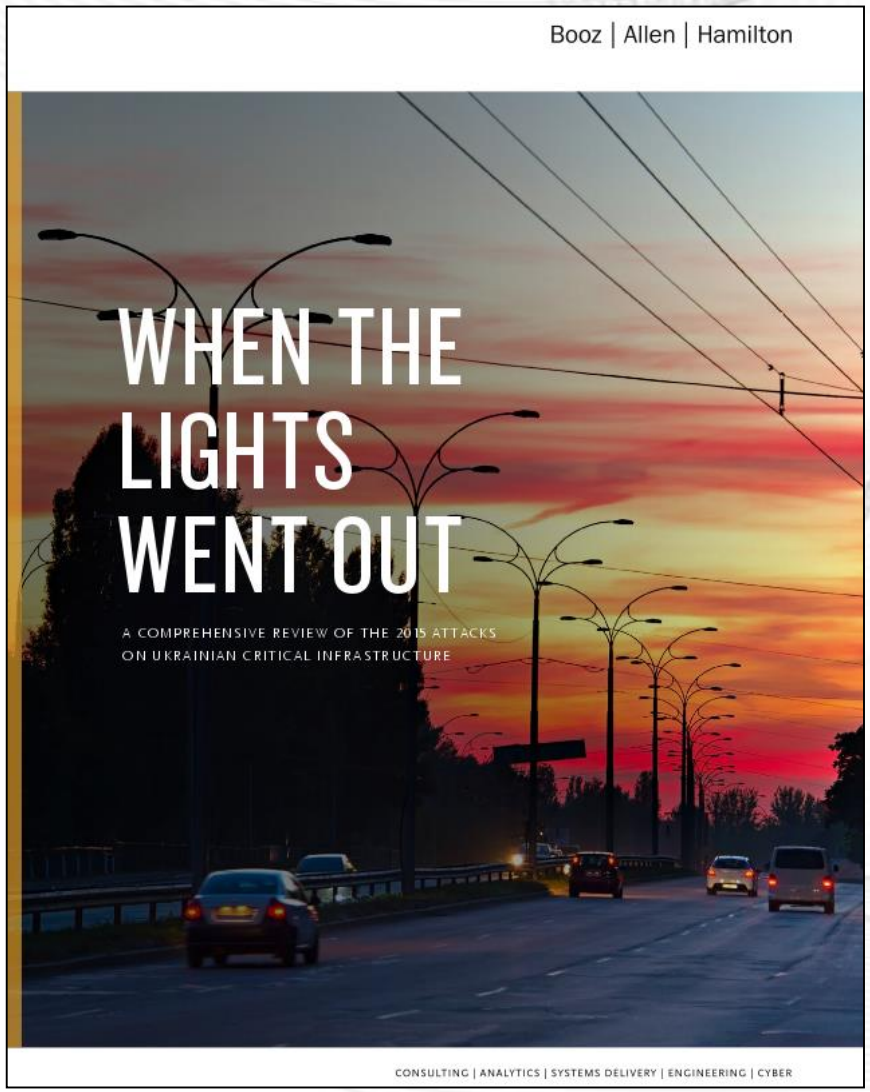
Visto il decreto legislativo 30 luglio 1999, n. 303, recante «Ordinamento della Presidenza del Consiglio dei ministri a norma dell'art. 11 della legge 15 marzo 1997, n. 59»;

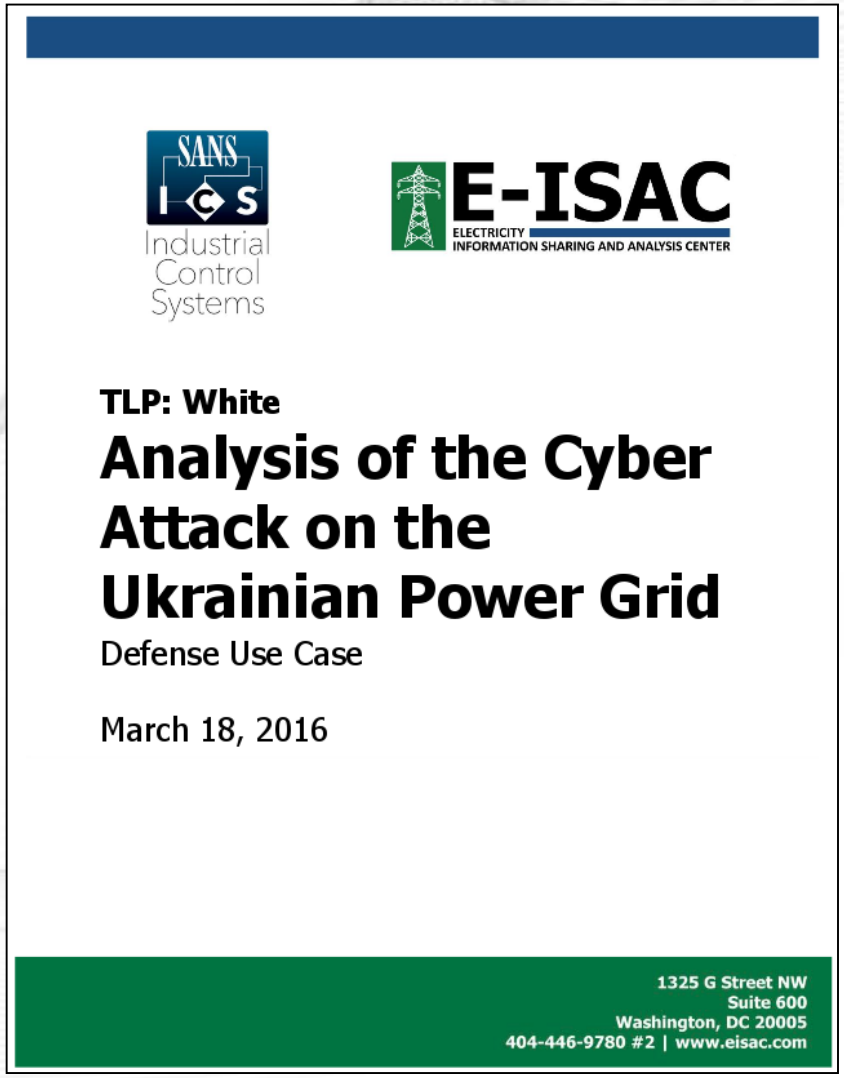
— 1 —

NATIONAL CYBER FRAMEWORK

Types of cyber treath:

- *Cyber-crime (ie: fraud);*
- *Cyber-espionage (ie: data theft);*
- *Cyber-terrorism (with ideological influence);*
- *Cyber-warfare (plan and conduct cyber operations).*


Booz | Allen | Hamilton
WHEN THE LIGHTS WENT OUT
A COMPREHENSIVE REVIEW OF THE 2015 ATTACKS ON UKRAINIAN CRITICAL INFRASTRUCTURE
CONSULTING | ANALYTICS | SYSTEMS DELIVERY | ENGINEERING | CYBER


SANS ICS Industrial Control Systems
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER
TLP: White
Analysis of the Cyber Attack on the Ukrainian Power Grid
Defense Use Case
March 18, 2016
1325 G Street NW
Suite 600
Washington, DC 20005
404-446-9780 #2 | www.eisac.com

Hacking link to USS McCain warship collision? Expert says 'I don't believe in coincidence'

THE collision of a second US warship this year that has left 10 sailors missing points to the possibility of cyber espionage, an expert has warned.

Charis Chang @CharisChang2

Fourth US Navy collision this year raises suspicion of cyber-attacks

by TRISTAN GREENE — 8 weeks ago in INSIDER

Credit: US Navy

Langner

To Kill a Centrifuge

A Technical Analysis of What Stuxnet's Creators Tried to Achieve

Ralph Langner

November 2013

Stuxnet

The Langner Group

Arlington | Hamburg | Munich

TARGET

- COMPANIES
- FINANCE
- ENERGY
- INSTITUTIONS (ECONOMY, TRANSPORT, HEALTH, DEFENCE)
- PEOPLE!!??

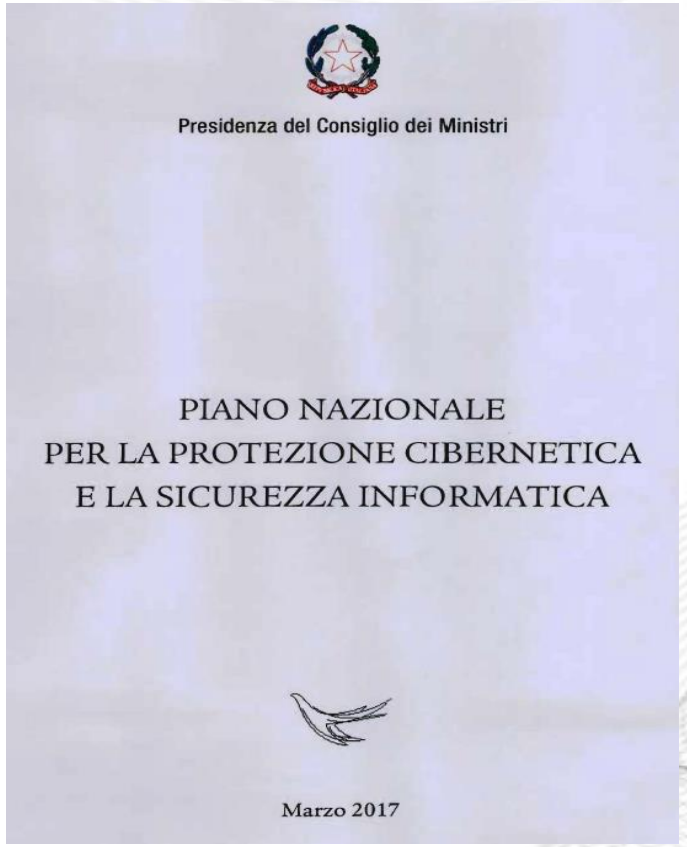
WHY

- NATIONAL STRATEGY
- POLITICS
- PROFIT
- SELF ACHIEVEMENT

WHO

- STATES
- TERRORISTS
- CRIMINALS
- HACKTIVISTS
- INFILTRATED

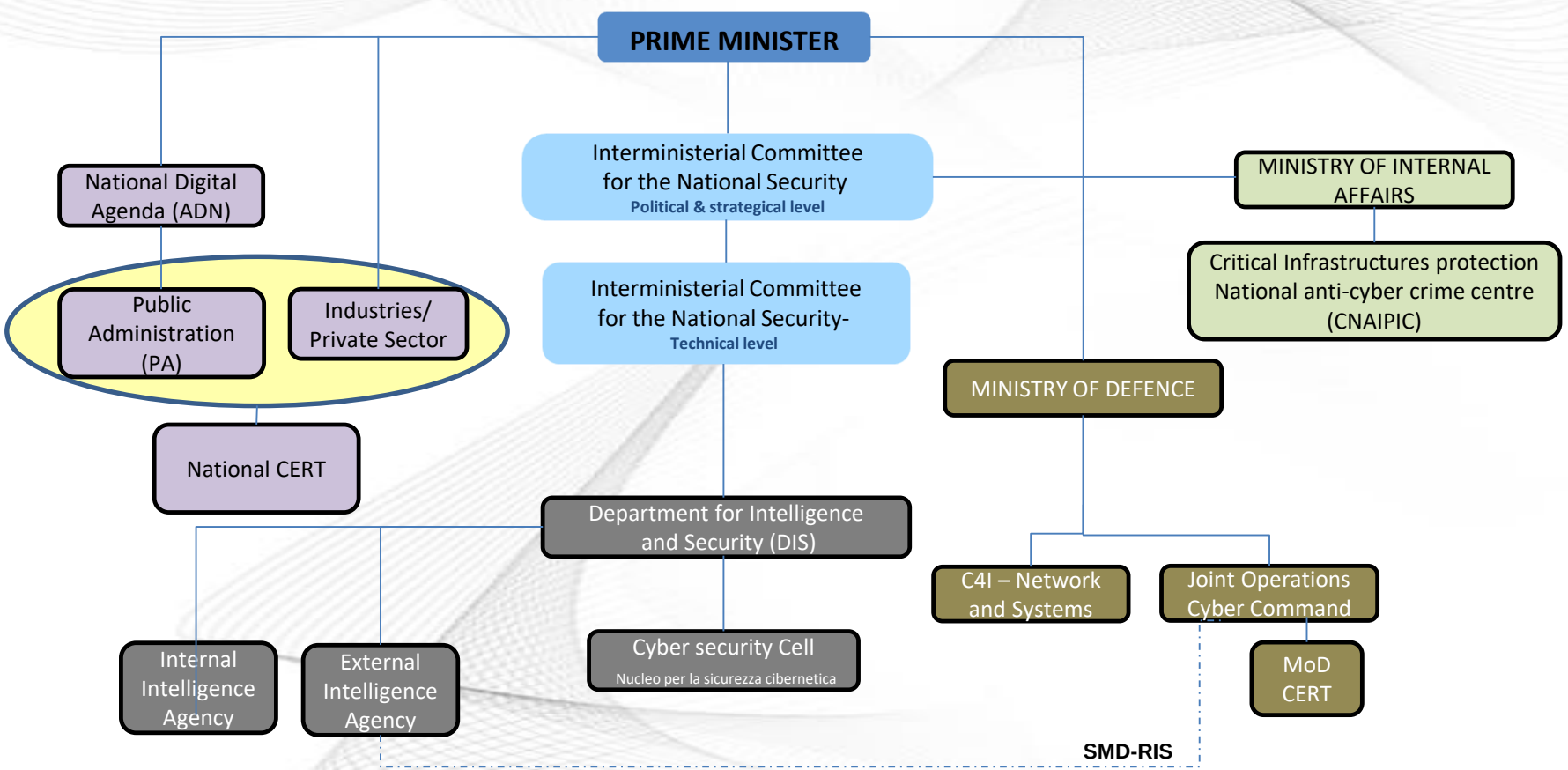
NATIONAL CYBER FRAMEWORK



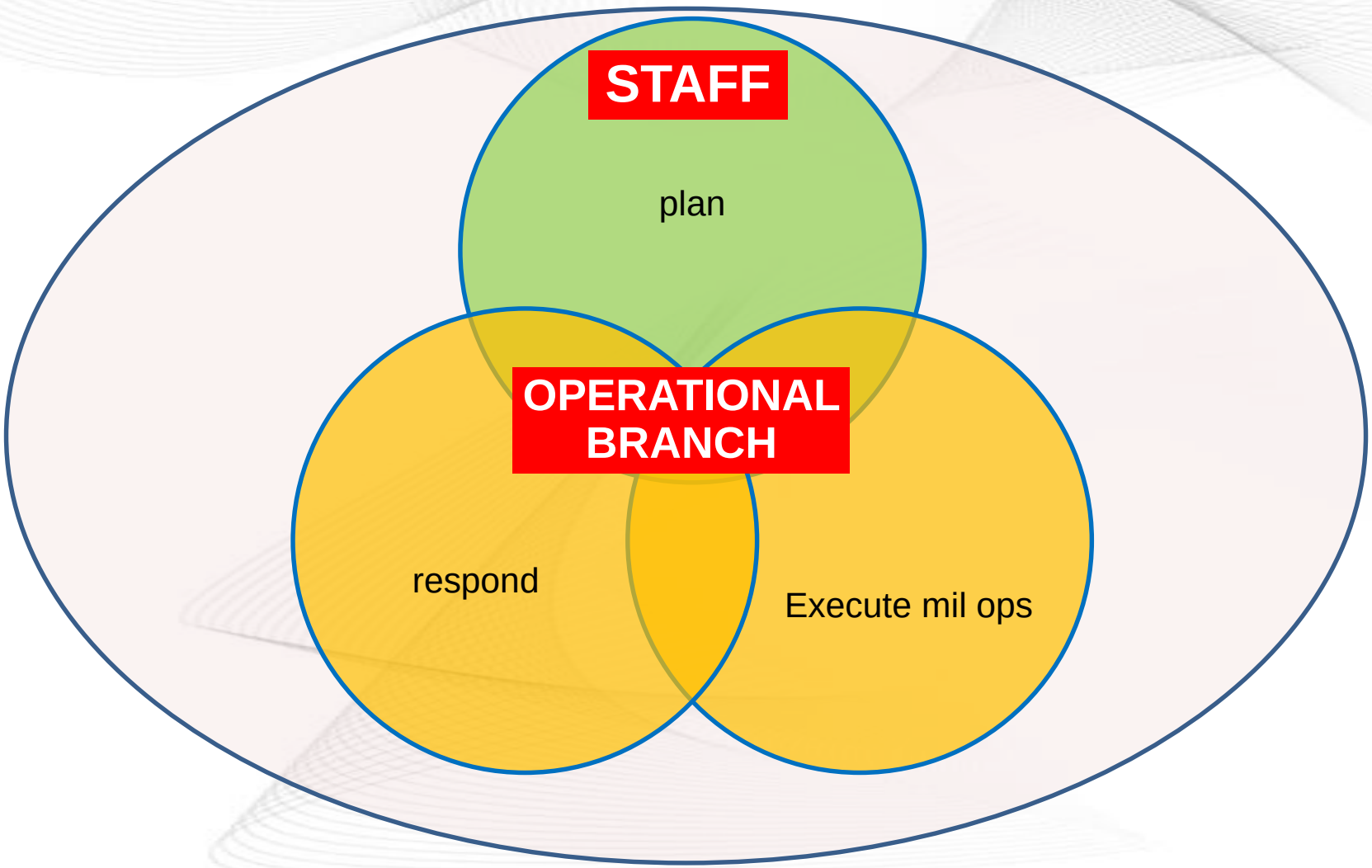
*p.12 - "Set up a **JOINT OPERATIONS CYBER COMMAND** to protect MoD networks and systems as well as to conduct cyber operations."*

p.15 - "Develop Command and Control Structures to plan and conduct military operations in the cyberspace."

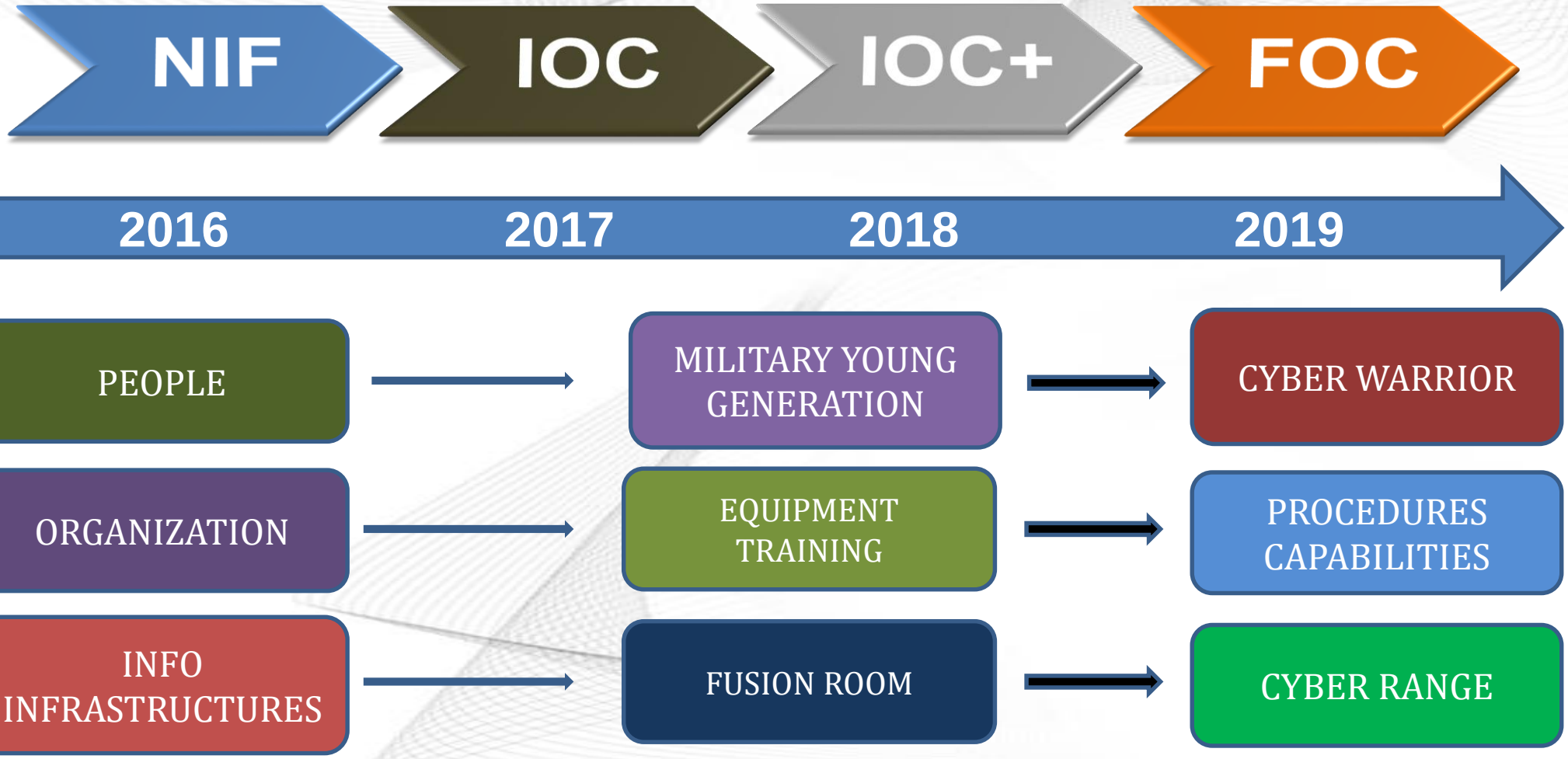
NATIONAL CYBER FRAMEWORK



CIOC



ITA JOCC


NIF
IOC
IOC+
FOC
2016
2017
2018
2019
PEOPLE
ORGANIZATION
INFO INFRASTRUCTURES
MILITARY YOUNG GENERATION
EQUIPMENT TRAINING
FUSION ROOM
CYBER WARRIOR
PROCEDURES CAPABILITIES
CYBER RANGE

CURRENT CYBER DEFENCE CAPABILITY

Joint Operations Cyber Command (JOCC)

Cyber Operations

***Computer Emergency Response Team* (CERT)**

C4 Defence Command (C4D)

Infrastructure C4D

***Security Operation Center* (SOC)**

***Infrastructure Operation Center* (IOC)**

***Network Operation Center* (NOC)**

To complete

***Cyber Defence* (CD)**

EDUCATION & TRAINING

education:

- Courses and masters *Cyber Defence* @ STELMILIT Chiavari;
- Courses *Cyber Operation* @ CIFIGE;

training:

- *Cyber Range* (STELMILIT Chiavari);
- *Cyber Lab* (CIOC).

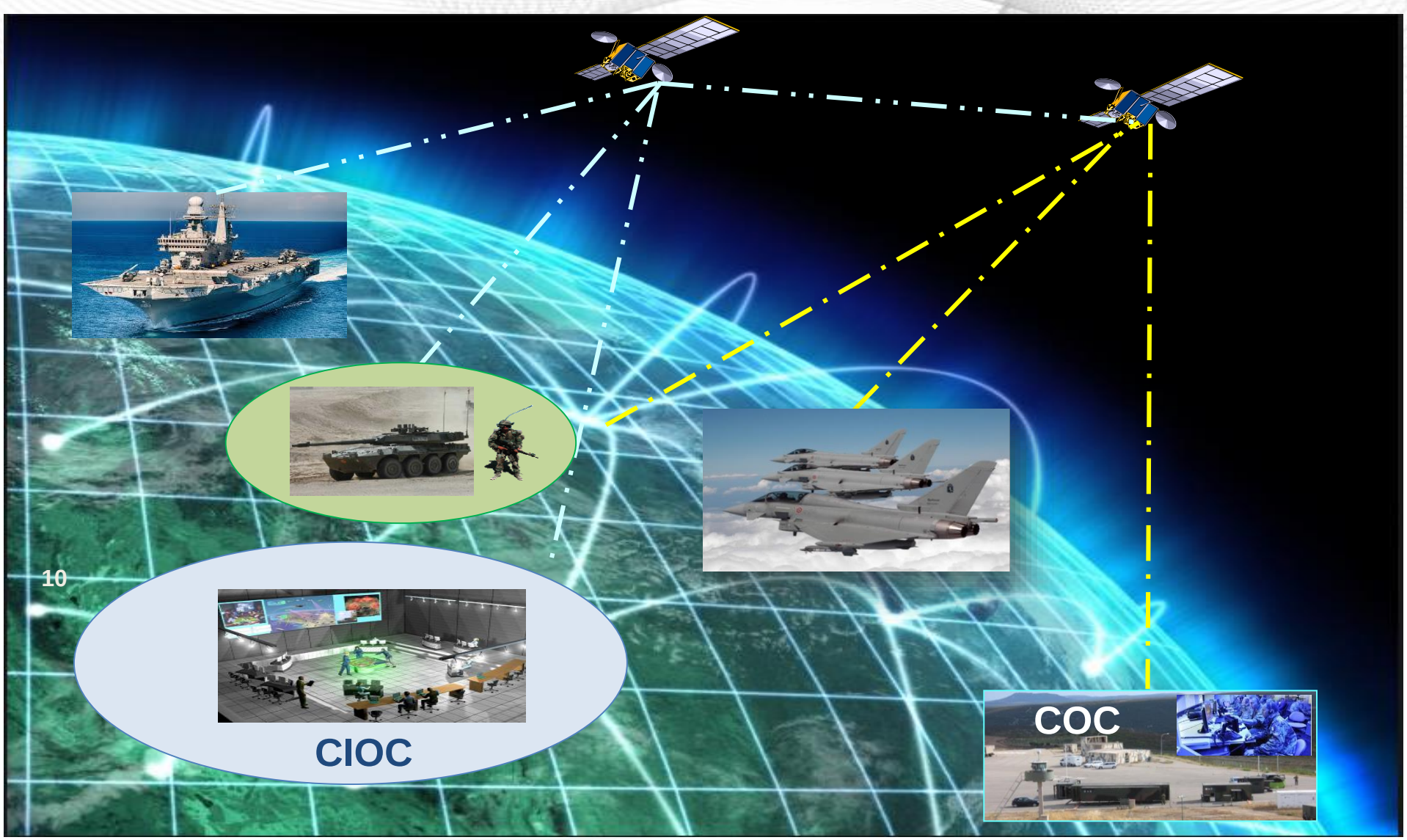
CYBER RANGE

- ✓ **Dual Use;**
- ✓ **Cooperation with secondary schools and universities →**

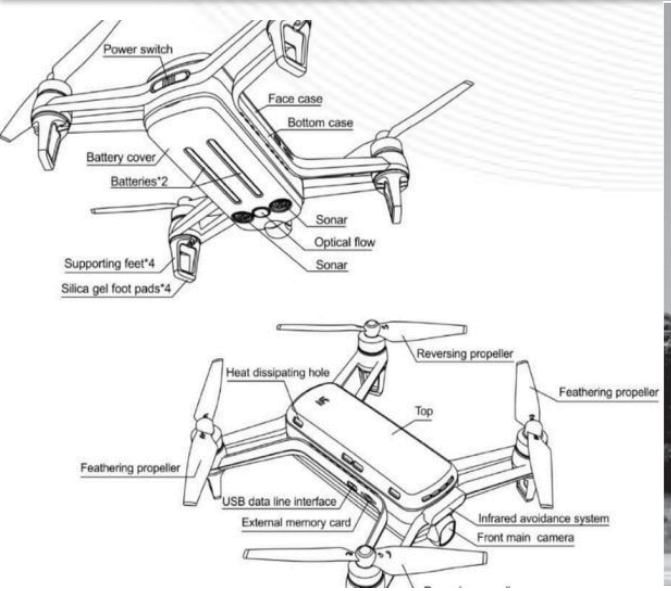
  <u>next generation of cyber</u>
  <u>defenders;</u>
- ✓ **New Job opportunities for former employed people;**

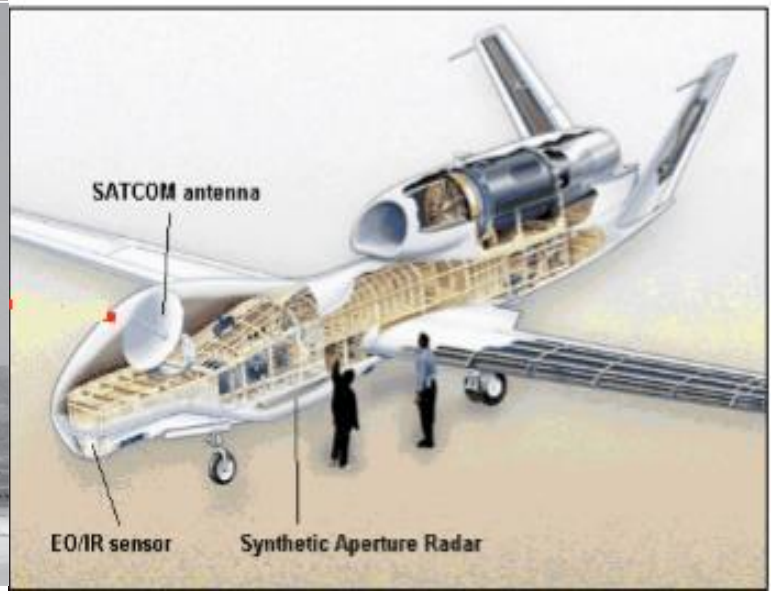
- ✓ **<u>Cyber Ecosystem development</u> between Defence, Industry and University/ Research Centers;**
- ✓ **Strategic asset to be developed for <u>Nation</u>.**

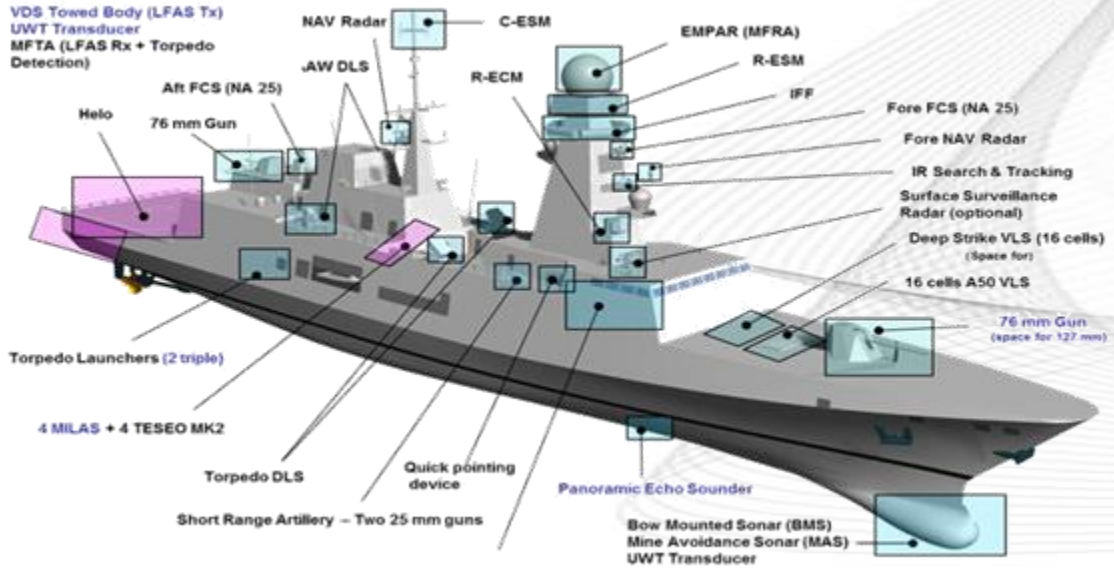
ITA JOCC MISSION

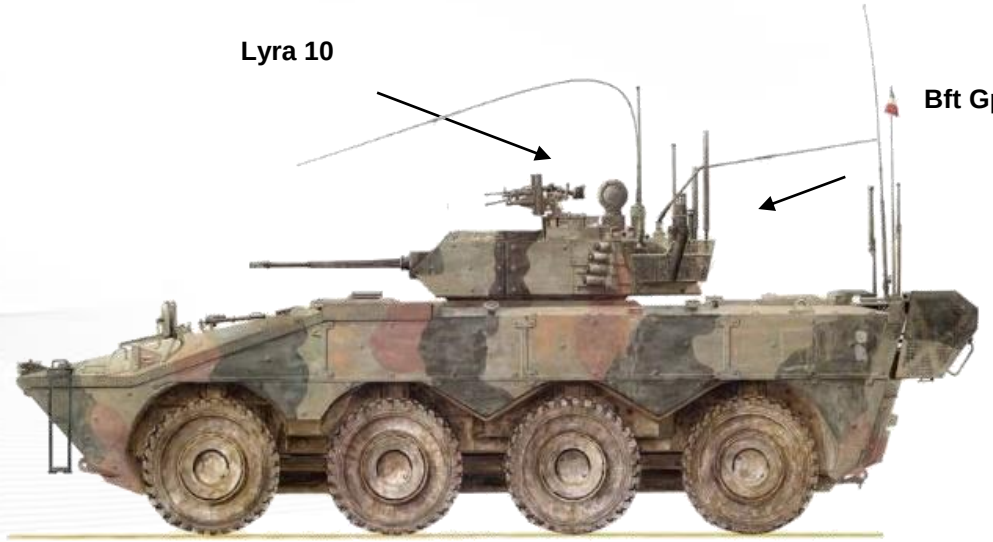


ITA JOCC MISSION

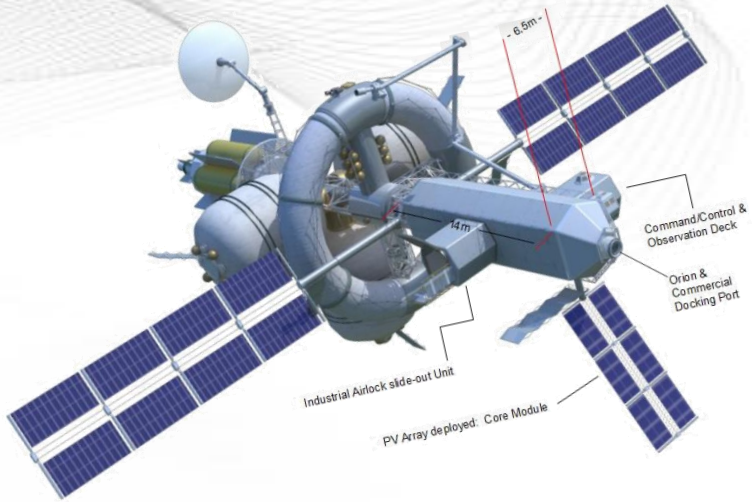






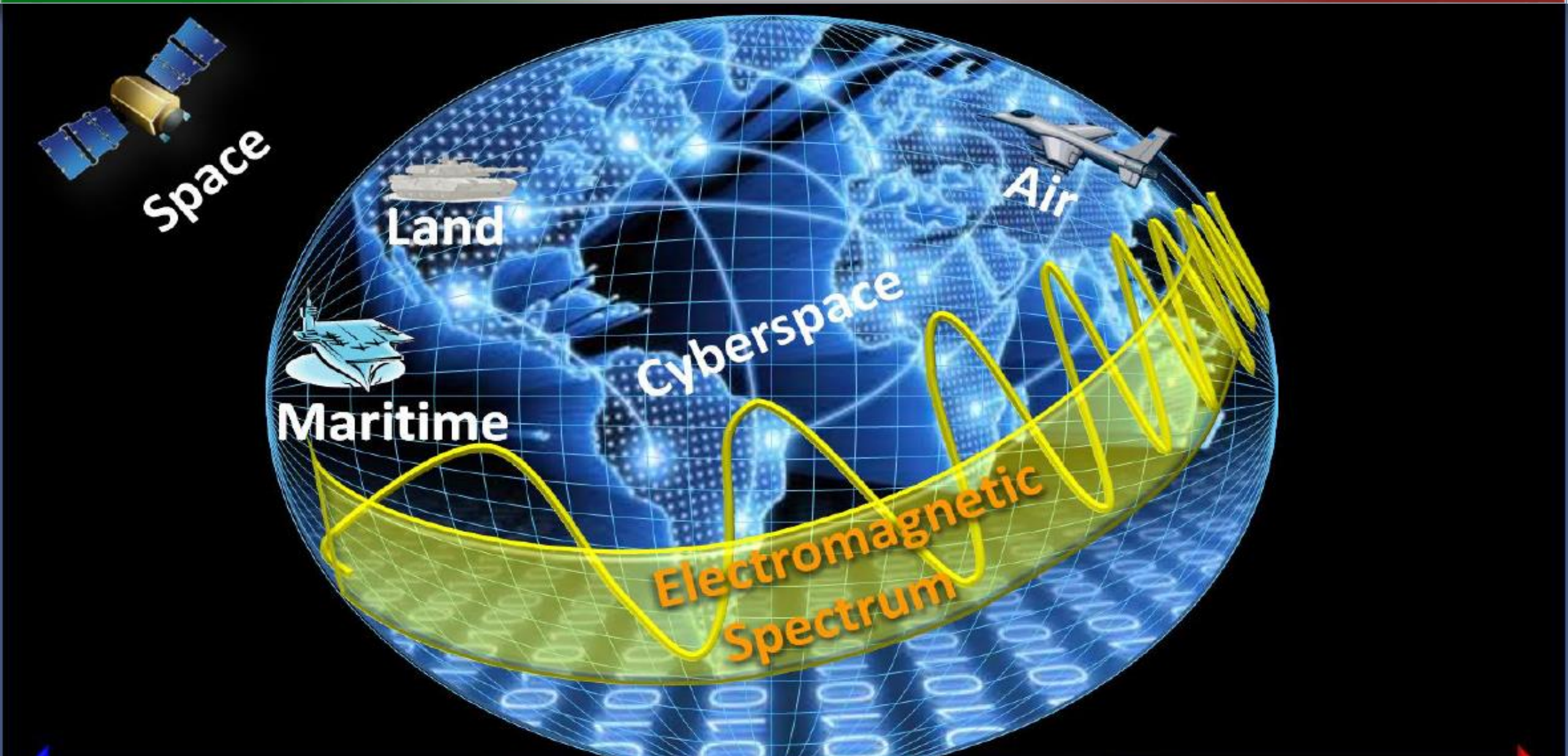


ITA JOCC MISSION



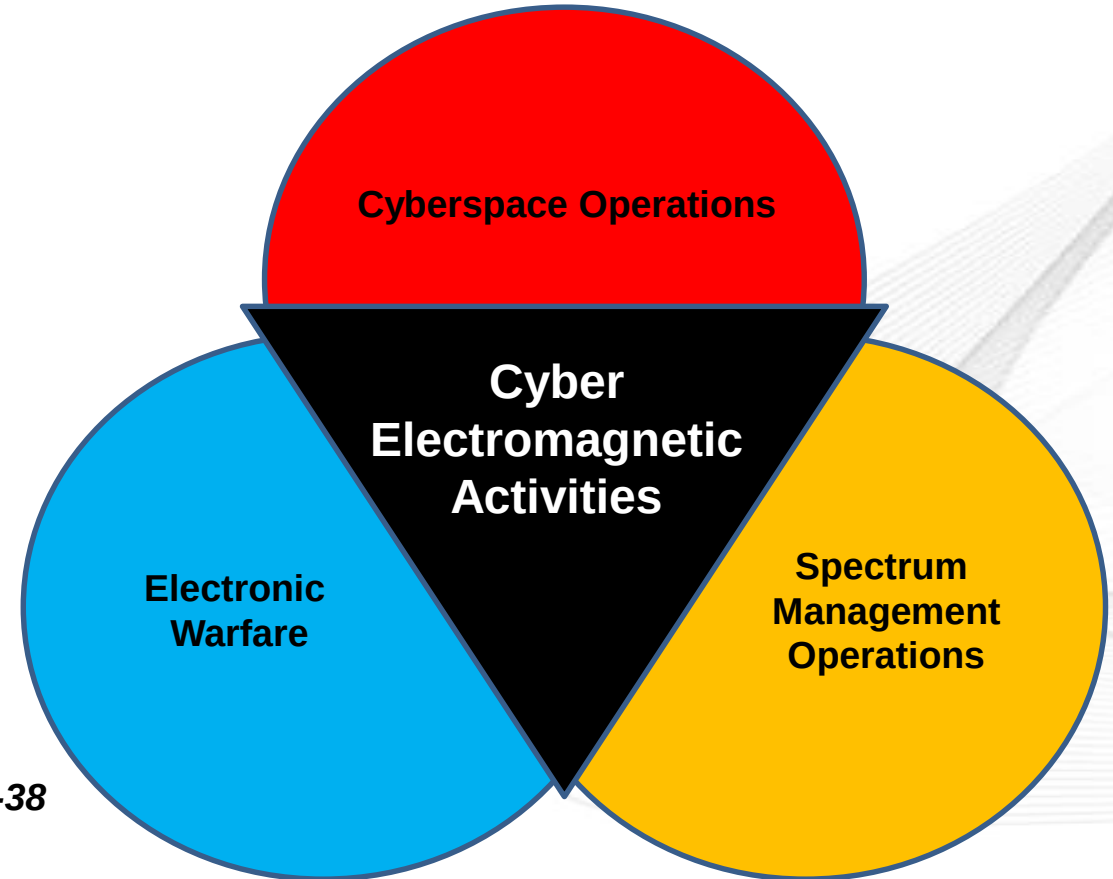
- ✓ *Satellite links;*
- ✓ *Ground Stations;*
- ✓ *GNSS (Global Navigation Satellite System).*

CYBER ELECTROMAGNETIC ACTIVITIES

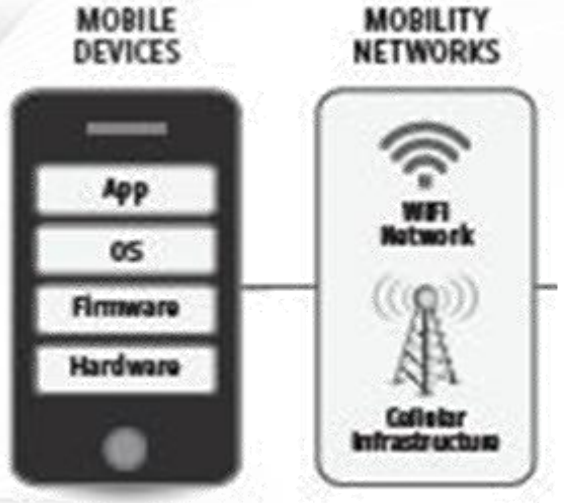


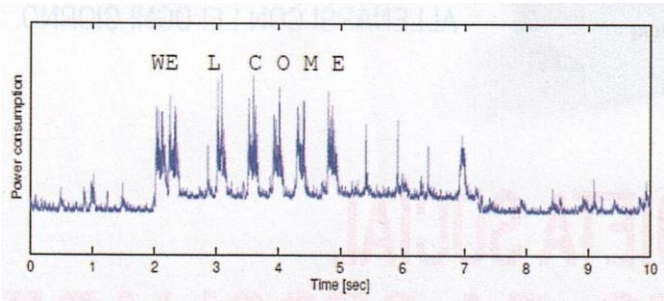
CEMA

Cyber electromagnetic activities are activities leveraged to seize, retain, and exploit an advantage over adversaries and enemies in both cyberspace and the **electromagnetic spectrum**, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system. (ADRP 3-0) The three components of **cyber electromagnetic activities** are **cyberspace operations, electronic warfare, and electromagnetic spectrum o**perations.



FM 3-38





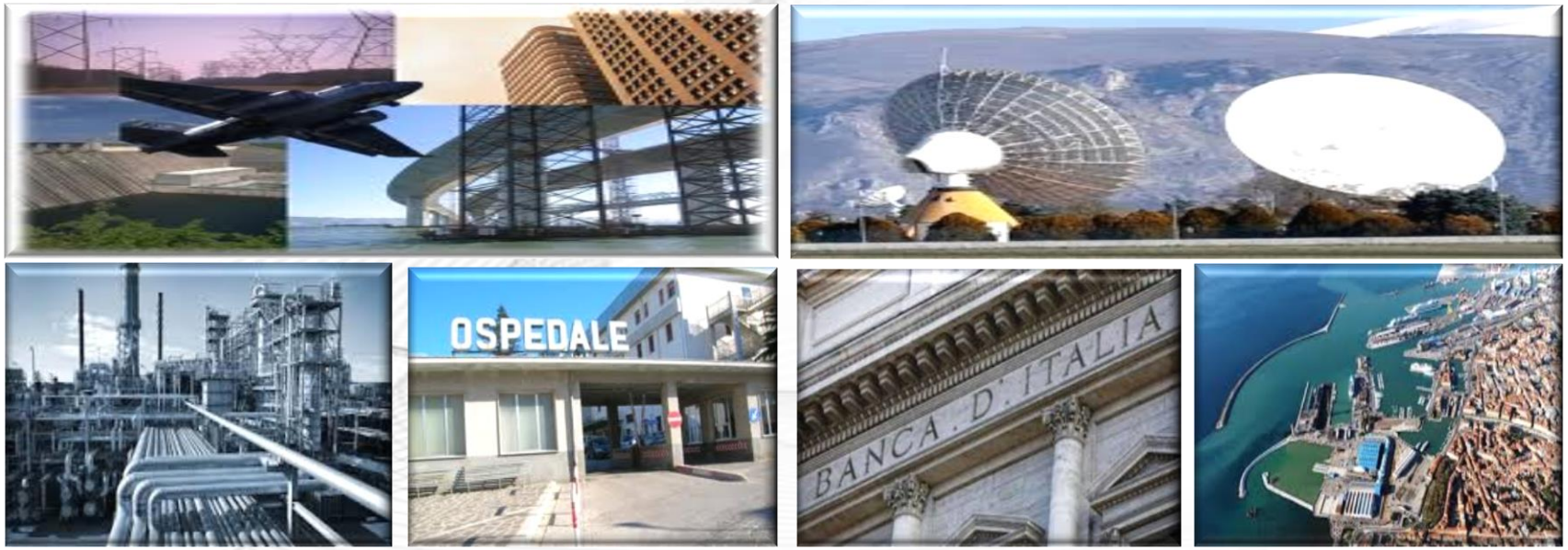
http://www.web-idea.it/

Cyber Operation center CyOC

NATO's cyber operations center will allow the Alliance to "respond more effectively" to cyber attacks by integrating cyber measures with conventional military capabilities".

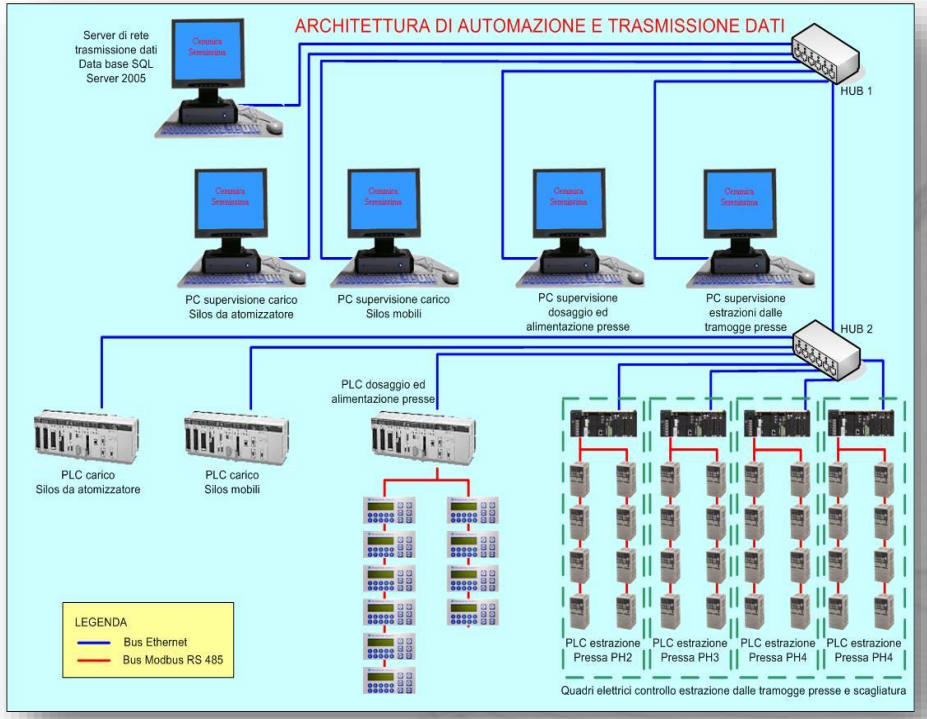

GOVERNMENT
Policy & Politics
Governance & Accountability
ARMY
Capability &
Effectiveness
PEOPLE
Legitimacy &
Sustainability

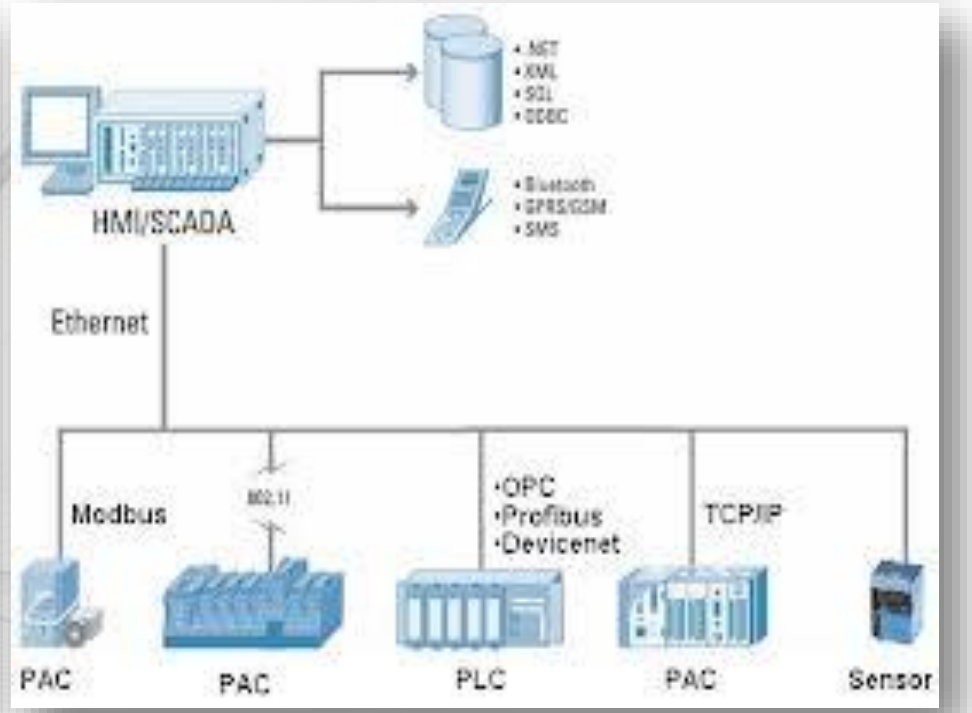
CRITICAL INFRASTRUCTURES



Critical infrastructures

Cyber Physical System (PLC, SCADA)





WHITE PAPER: CUTTING THROUGH THE HYPE

Advanced Persistent Threats: A Symantec Perspective

Preparing the Right Defense for the New Threat Landscape

Content

APT28 SUMMARY

APT28 is an adversary group which has been active since at least 2007. This group was identified to be targeting mostly military or government entities and has been linked publicly to intrusions into the German Bundestag [1], France's TV5 Monde TV station in 2015 [2] and the DNC [3] in April 2016. The incidents linked to this group have been analyzed by different security companies and independent researchers. These companies label already discovered and named APT Groups with their own name convention. Therefore, the group is also known as "Sofacy", "Fancy Bear", "Sednit", "Pawn Storm", "TsarTeam" and "Strontium".

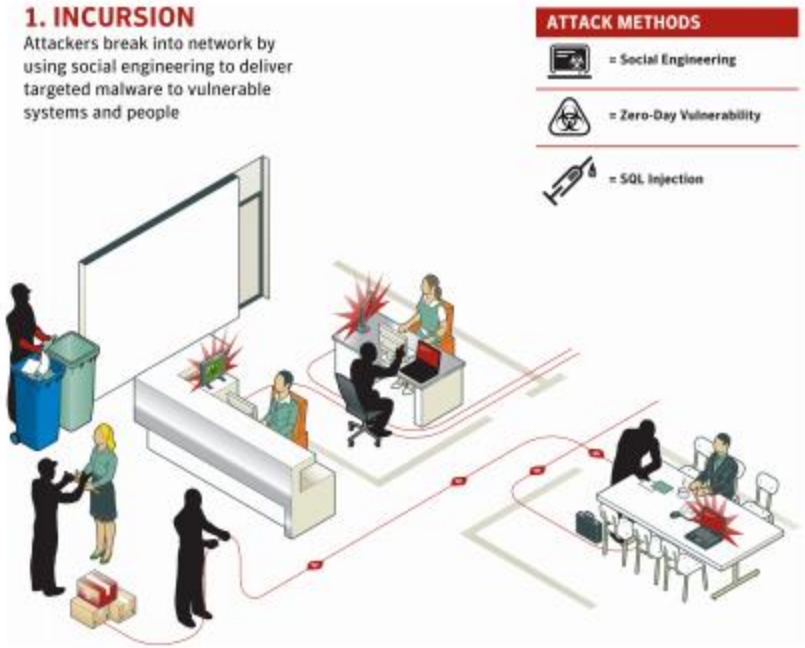
APT 30 SUMMARY

- The threat actor named as APT30 by FireEye is considered to be speaking Chinese. The language artifacts can be found by analyzing the metadata and the user interface of the malware used by APT30. The list of confirmed targets consists of companies and organizations in various fields operating in India, South Korea, Malaysia, Vietnam, Thailand, Saudi Arabia and United States. In addition to the confirmed countries, other countries in the region, like Singapore, Myanmar, Japan, etc., are also suspected to be targeted by the APT30 group

It should now be evident that although not every organization is a likely target of an APT, they are a real and serious threat to some organizations. Additionally, any organization can benefit from better understanding of APTs, because APT techniques are likely to be adopted over time by mainstream hackers and cybercriminals. Finally, since anyone could be the object of a targeted attack—and APTs are examples of highly advanced, long-term, and large-scale targeted attacks—if you have a better understanding of APTs, you can better defend your organization against targeted threats of any kind.

How do APT attacks work?

APT attacks are carefully planned and meticulously executed. They typically break down into four phases: incursion, discovery, capture, and exfiltration. In each phase a variety of techniques may be used, as described below.



Phase 1: Incursion

In targeted attacks, hackers typically break into the organization's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods. These methods are also used in APTs, often in concert. The main difference is that while common targeted attacks use short-term, "smash and grab" methods, APT incursions are designed to establish a beach head from which to launch covert operations over an extended period of time. Other characteristics of APT incursions include the following:

- **Reconnaissance**—APT attacks often employ large numbers of researchers who may spend months studying their targets and making themselves familiar with target systems, processes, and people, including partners and vendors. Information may be gathered both online and using conventional surveillance methods. In the case of the Stuxnet attack on organizations believed to be operating Iranian nuclear

Phase 1: Incursion

In targeted attacks, hackers typically break into the organization's network using social engineering, zero-day vulnerabilities, SQL injection, targeted malware, or other methods. These methods are also used in APTs, often in concert. The main difference is that while common targeted attacks use short-term, "smash and grab" methods, APT incursions are designed to establish a beach head from which to launch covert operations over an extended period of time. Other characteristics of APT incursions include the following:

- **Reconnaissance**—APT attacks often employ large numbers of researchers who may spend months studying their targets and making themselves familiar with target systems, processes, and people, including partners and vendors. Information may be gathered both online and using conventional surveillance methods. In the case of the Stuxnet attack on organizations believed to be operating Iranian nuclear

3-Martin Lee, "Repeat Attacks Betray Attackers' Motivations," Symantec, July 13, 2011

facilities, the attack team possessed expertise in the design of the programmable logic controllers (PLCs) used for uranium enrichment that were targeted in the attack.[4]

- **Social engineering**—Incursion is often accomplished through the use of social engineering techniques, such as inducing unsuspecting employees to click on links or open attachments that appear to come from trusted partners or colleagues. Unlike the typical phishing attack, such techniques are often fed by in depth research on the target organization. In one case, a small number of human resource employees were targeted using an apparently innocuous attachment, a spreadsheet on hiring needs that appeared to come from a job listing website. In the case of Hydraq, targeted users were led to a picture-hosting website where they were infected via a drive-by-download.
- **Zero-day vulnerabilities**—Zero-day vulnerabilities are security loopholes that are unknown to the software developer and may therefore be exploited by attackers before the developer can provide a patch or fix. As a result, the target organization has zero days to prepare; it is caught off-guard. Since it takes significant time and effort to discover zero-day vulnerabilities, only the most sophisticated attacker organizations are likely to take advantage of them. APTs often use one zero-day vulnerability to breach the target, switch to a second and then a third as each point of attack is eventually fixed. This was the case with Hydraq. The Stuxnet attack was exceptional in that four separate zero-day vulnerabilities were exploited simultaneously.
- **Manual operations**—Common or massive attacks employ automation to maximize their reach. "Spray and pray" phishing scams use

108 customer reviews | 47 answered questions

Price: $55.50

In Stock.

Arrives before Christmas. Choose delivery option in checkout.

This item ships to **Italy**. **Want it Monday, Dec. 18?** Order within **4 hrs 57 mins** and choose **AmazonGlobal Priority Shipping** at checkout. Learn more

Sold by DBROTH and Fulfilled by Amazon.

- 4MB flash memory stores 2000 pages of text
- Work great with all wired USB keyboards and work with all versions of Windows and Linux
- No software or drivers needed
- National keyboard layout support

Product description

records everything typed on a [illegible] keyboard. Absolutely no software is required and ... is completely invisible ... any software. The ... USB is the stealthiest hardware keylogger in existence - it is impossible to detect!

0 votes

Question: If the logger is attached it will log the windows password too?

Answer: Yes. If it is typed on the attached keyboard, it will be recorded.

By Doug Kerfoot on July 26, 2014

...on't.

...B port and

0 votes

Question: Will this work with a wireless keyboard & mouse combo?

Answer: Yes, as long as the keyboard and mouse is connected via bluetooth to the computer your trying to key log.

By Giselle R on February 22, 2017

0 votes

Question: What if the OS has an administrative lock on it? Like on a windows computer where you need to enter administrative password to do any basic things?

Answer: This USB works directly with the keyboard, the OS's Lock its irrelevant. All that is typed into the PC or MAC pass trough this Device then the PC or MAC O...

By Michael Kings on October 25, 2014

See all 3 answers

- Dispositivo audio integrato con microfono;
- Scheda SIM;
- Rilevabile solo se si smonta il mouse;
- Attivo fino a 2 ore dopo che il pc è stato spento.

- Presa schuko per monitaraggio consumi;
- Collegata via wireless e/o bluetooth;
- Gestione via app;
- Tentativi di accesso a circa 200 domini.

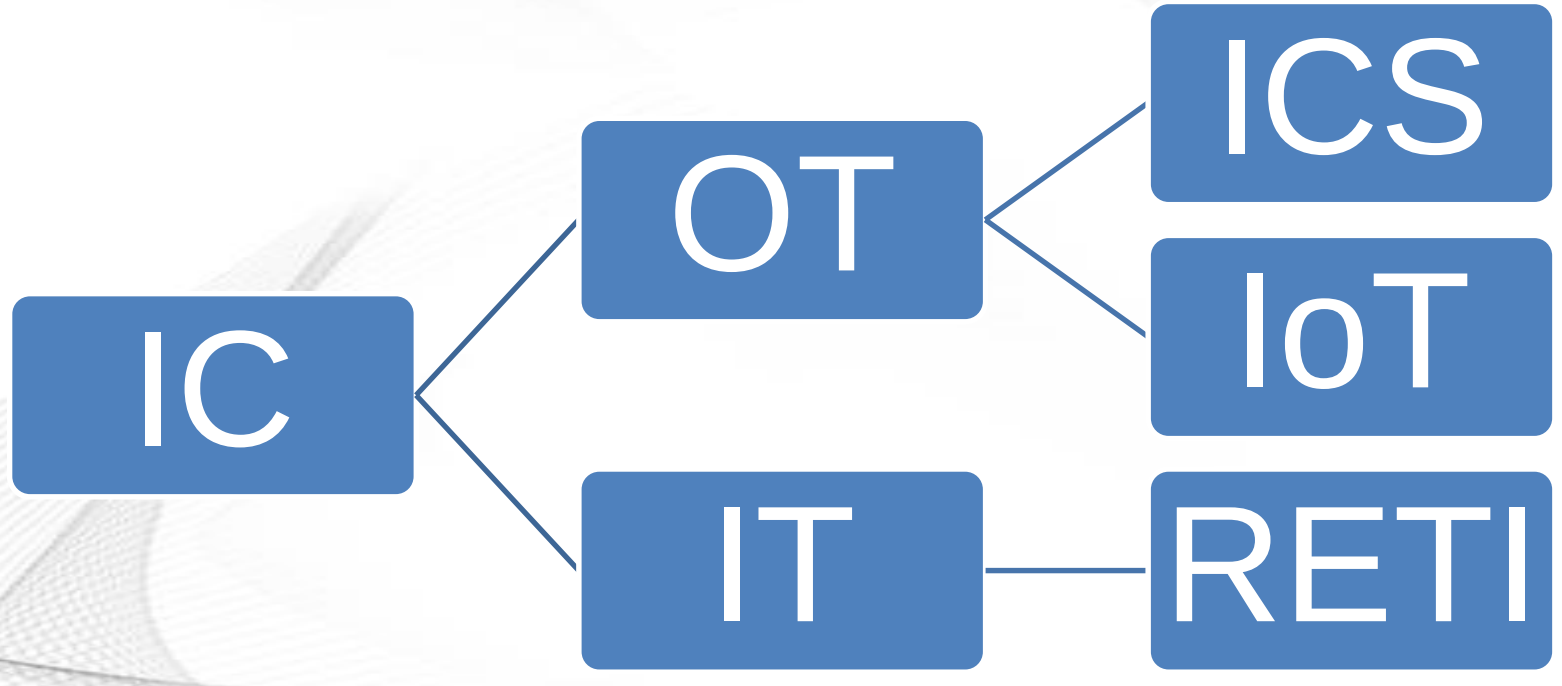

struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *groups_alloc(int gidsetsize){
struct group_info *group_info;
int nblocks;
int i;
nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
/* Make sure we always allocate at least one indirect block pointer */
nblocks = nblocks ? : 1;
group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
if
gro
gro
ato
if (gidsetsize <= NGROUPS_SMALL)
group_info->blocks[0] = group_info->small_block;
else {
for (i = 0; i < nblocks; i++) {
gid_t *b;
b = (void *)__get_free_page(GFP_USER);
if (!b)
goto out_undo_partial_alloc;
group_info->blocks[i] = b;
ACCESS DENIED

FREE OF MOVEMENT IN THE DIGITAL DOMAIN

MILITARY

of

THINGS



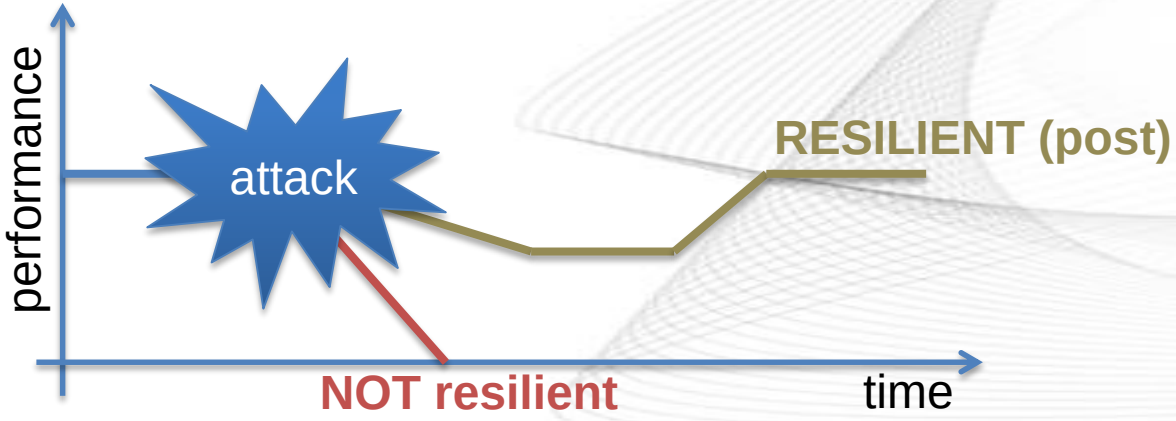
ITA JOCC MISSION

"The 2 key words for Italian Defence":

(Elisabetta TRENTA - Minister of Defence)

1 RESILIENCE

*Resilience as the ability to **prepare for** and **adapt** to changing conditions and **withstand** and **recover** rapidly from **disruptions**.*
*Resilience includes the ability to **withstand and recover from deliberate attacks**, accidents, or naturally occurring threats or incidents."*
[https://www.dhs.gov/what-security-and-resilience]



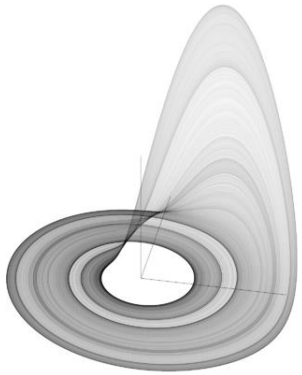
2 DUAL USE

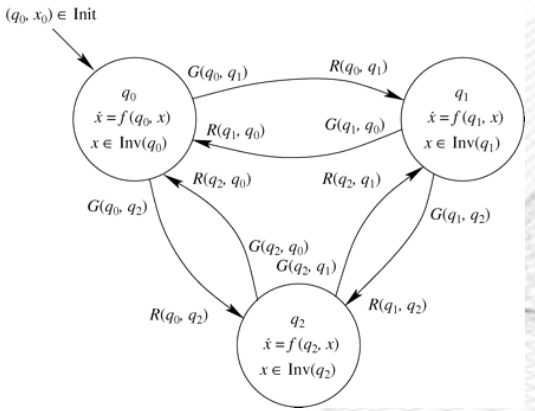
- *Develop **Cyber Ecosystem** between Defence, Industry and University/ Research Centers*
- ***Energy Security – Cyber Security***

ITA JOCC MISSION

$$\int_a^b f'(x)\,dx = f(b) - f(a)$$

$$\frac{d}{dx}\int_a^x f(t)\,dt = f(x)$$





IST-152 Workshop on **Intelligent Autonomous Agents for Cyber Defence and Resilience**

Industrial Control System: Comprehensive Security Approach

SUPPORT PAPER

AUTHORS

PANICO, AGOSTINO – "LA SAPIENZA" UNIVERISTY OF ROME
CERULLO, LUCIO – JOINT OPERATIONS CYBER COMMAND - JOCC
DELAURENTIS, VITO – JOINT OPERATIONS CYBER COMMAND - JOCC
MURINO, GIUSEPPINA – UNIVERSITY OF GENOVA
VESTITO, GEN. FRANCESCO – JOINT OPERATIONS CYBER COMMAND - JOCC

Perspectives on Cyber Operations

BG (AF) Francesco VESTITO
JOCC Commander

Rome, 25th March 2019