Cyber Defense: three fundamental steps

Giorgio Mosca
Strategy and Technology Director

LEONARDO
SECURITY & INFORMATION SYSTEMS

“It would seem that Caesar's recurrent and deep-rooted fault was his concentration in pursuing the objective immediately in front of his eyes to the neglect of his wider object. “
— B.H. Liddell Hart, Strategy

In 5 years

4B
Users 2019

5.9B
Smartphone Connections 2020

44 ZB
Data zettabytes in 2020

24.4B
IP-connected devices 2019

200B
IoT Devices 2019

159 B$
Global public cloud market 2020

168 EB
Exabytes/month in IP traffic in 2019

0
Downtime & Latency request

The future

Physical and Digital worlds overlapping at an unprecedented rate

Biotechnologies, blockchain, nanotechnologies, robotics, 3d printing, cyber-physical systems, massive usage of augmented reality and artificial intelligence.

Societies will be a networked cyber physical ecosystem of services, systems, people, information

Low investments, limited risks, disruptive effects. Whatever the objective, the cyber option will be more and more appealing for hostile entities.

Some signals

Digital Trust is first inhibitor factor to UE Digital Single Market

Connected everything fuels the emergence of new attack vectors

NATO declared Cyber the 5th Battlespace domain

Cyber is a main point in most of Nations and Board Rooms' Agendas.

Impacted sectors

Transport
Autonomous systems, Situational awareness

Security
Drone technology, Weapon systems, Situational awareness

Energy
Smart grid and innovative EMS/DMS

Healthcare
Smart medical devices, Big data. robotics

Banking
Blockchain technology

The question

How to manage this complexity for scenarios like Terrorism, Cybercrime, Immigration Flows and Border control, Protection and Resilience of Transportation, Communications, Energy, Manufacturing ?

How to build / maintain TRUST?

The world

- Italy under strong cyber espionage
- Attacks to Ukraine Crtical Infrastructures
- US claim Russians attacks to presidential elections
- Turkey claims US attacks to Crtical Infrastructures
- Saudi claims Iranian malware attacks
- Estonia, Georgia, Moldavia, Crimea, …
- Scandinavia: Air Traffic Management, Railway Ticketing, Comms & Telco

Will Cyber War take place?

TECHNOLOGICAL EVOLUTION

- the infrastructure available to armed forces encompasses cyber-physical systems, autonomous systems, intelligent sensors, satellite and wireless, new applications…

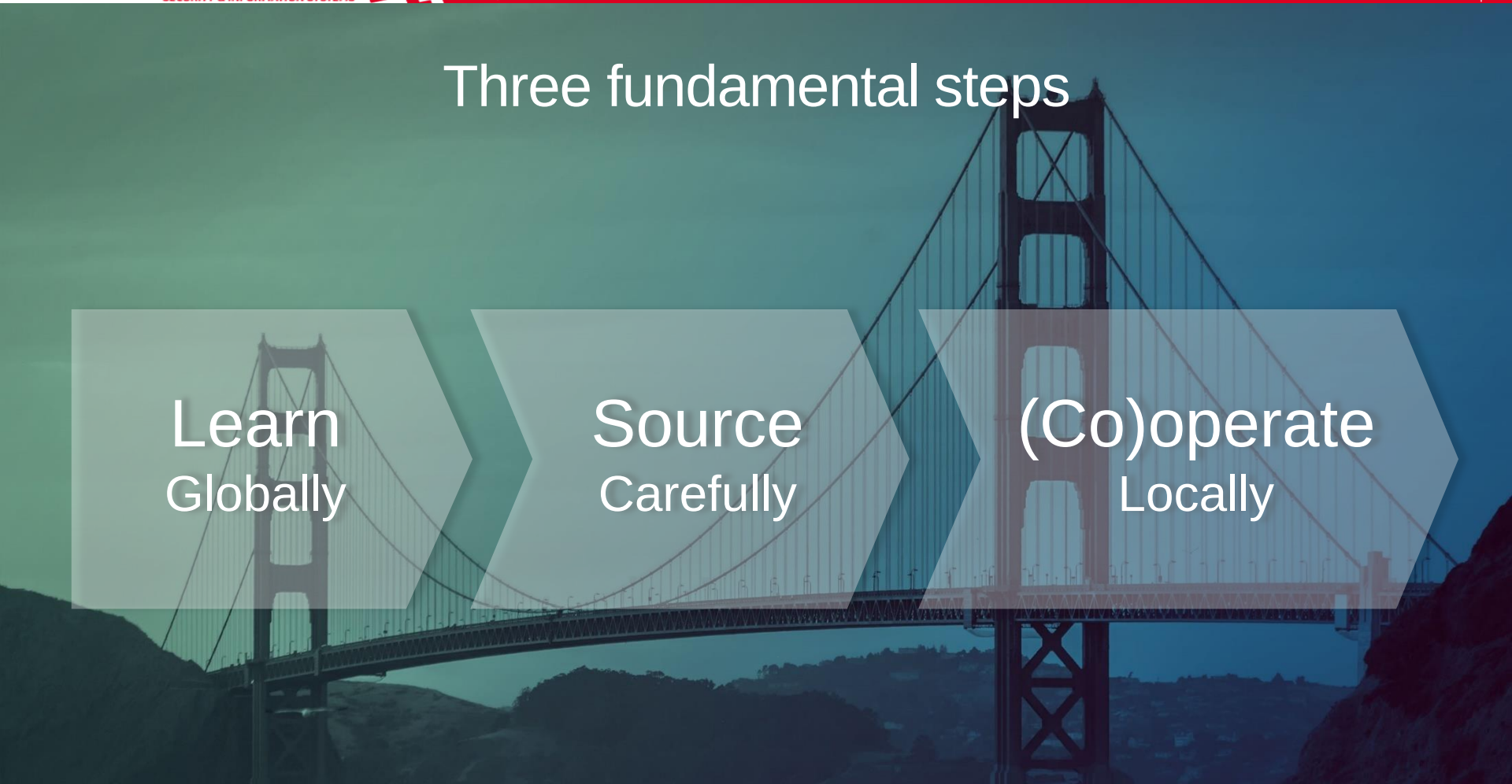
STRATEGIC EVOLUTION

- After the Warsaw Summit for NATO cyberspace will become, practically, an operating theatre
- Computer Network Operations (CNO): not only defense, but real active military operations in Joint & Combined scenarios
- Promotion of collective defense & reaction

CYBER WARFARE

- the use of electronic technologies, computer and telecommunication systems to harm the interests and infrastructures of a country, at large

Three fundamental steps



A global threat management issue

- Cyber crime has an estimated global impact of 400B$ per year
- What's the real technological and operational impact of state-sized threats?
- More and more frequently we hear suspicion of government actors… which consequences?
- Are only nations the possible origin of “state sized” threats?
- Global threats require shared intelligence. The private sector shares intelligence embedding conclusions in products… what else is required?
- How to approach threats (terrorism, serious attacks) using cyber space to create a transnational coordination and distributed attack capabilities?

The "bad guys" have already gone beyond national borders, with a pragmatic approach, to maximize attack power, "good guys" need to do the same.

Learn Globally

If we look at large countries, they are

- building digital defense strategies,
- developing distributed capacity,
- improving technological sectors,
- dedicating relevant portions of their operational, research and law enforcement forces to cyber

International scenario

European Commission initiatives with the NIS, the role of ENISA and EDA, the network of national CERT, the Constitution of the European Cyber Security Organization (ECSO)

Information exchange,

Cyber situational awareness and Intelligence unified Platforms (eg. NCIRC) exchange of information (eg. NCIRC vs CERT-EU)

Strategic evolution

UK 2016-2021 plan (Defend, Develop, Deter), France and Germany Cyber Commands China and Russia are very active

Value Chain & Supply Chain issues

- Strengthen and shorten the technological value chain by encouraging through all possible instruments the creation and/or the return of actual technological value in the EU area

- Need for creation of (costly) skills and abilities that are quite rare; promote science, technology and innovation → less finance and more engineers? less bureaucracy and more results?

- Value chain & Supply chain resilience : global chains are unavoidable, but we must have a plan to be resilient and react.
  Yesterday it was energy and some utilities, today "essential services" are many more and by 2018 with NIS we will tell everybody what they are…

Source carefully

Build a "Trust Circle" among Security System Integrators, the Cyber Community and all the Customers

"Strongly encourage" the (foreign) technology providers to cooperate according to shared rules

Both points are driven by the need to gain visibility of the real behavior of security tools

Cyber Community

needs to cooperate with a new set of stakeholders, providers and end-users, with technological assets becoming suddenly correlated

Security Process

follows and somehow leads the Customers in measuring its exposure and building its security process and capabilities

Security Services

shift from buying technologies to renting capabilities. Keep the pace of the evolution.

Cyber Technology Partners

manage (firmly) a liquid ecosystem of technologies and technology partners

Develop on focused technologies and exchange

Plan for the worst

Many Nations are organizing efforts from the point of view of attack and defense.

In various States, there is a tendency to increase the resilience of country Infosphere considering acts of war on a large scale.

Some examples:

- Various countries are studying a super national DNS able to keep running the overall infrastructure in the event of a crash, accidental or planned, of the global DNS network

- UK is developing a strategic plan to increase the resilience of the digital ecosystem to the invasion of the country Infosphere.

(Co)operate locally

Change
acquire concepts such as deterrence, active defense operations and strengthen government institutions like the CIOC and the CCE

Standards
revision of rules of acquisition to ensure greater timeliness and confidentiality

Strategy
structure with qualified domestic partners
a long term program to strengthen the Infosphere

Resources
Recognize qualified resources devoted to capacity building of national defense

A concrete proposal for a national program

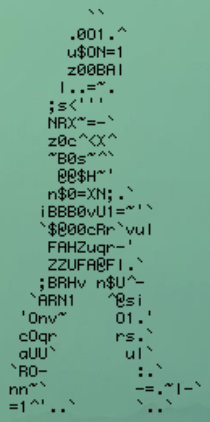
1. rationalization of infrastructures
2. deterrence capacity development
3. strengthen cyber security centers
4. create advanced cyber intelligence
5. increase the resilience of systems
6. control the vulnerabilities of CNIs
7. cyber-range & cyber academy
8. testing labs for COTS and technologies
9. constant research and training
10. collaboration among Institutions, Industry and Academia

Leonardo: targeting European Excellence in Cyber Industry

Being a solid cornerstone of the Cyber Security trust ecosystem in the EU

Developing technologies to detect and react: Machine Learning, Prediction models, Human Intelligence integration, …

Integrating cyber in products such as: RPAS – UAAS, Situational awareness, Unmanned Vehicle Control, Avionics – Traffic Control Security, Energy Grids



Thank you for your kind attention

Giorgio Mosca
giorgio.mosca@leonardocompany.com
leonardocompany.com