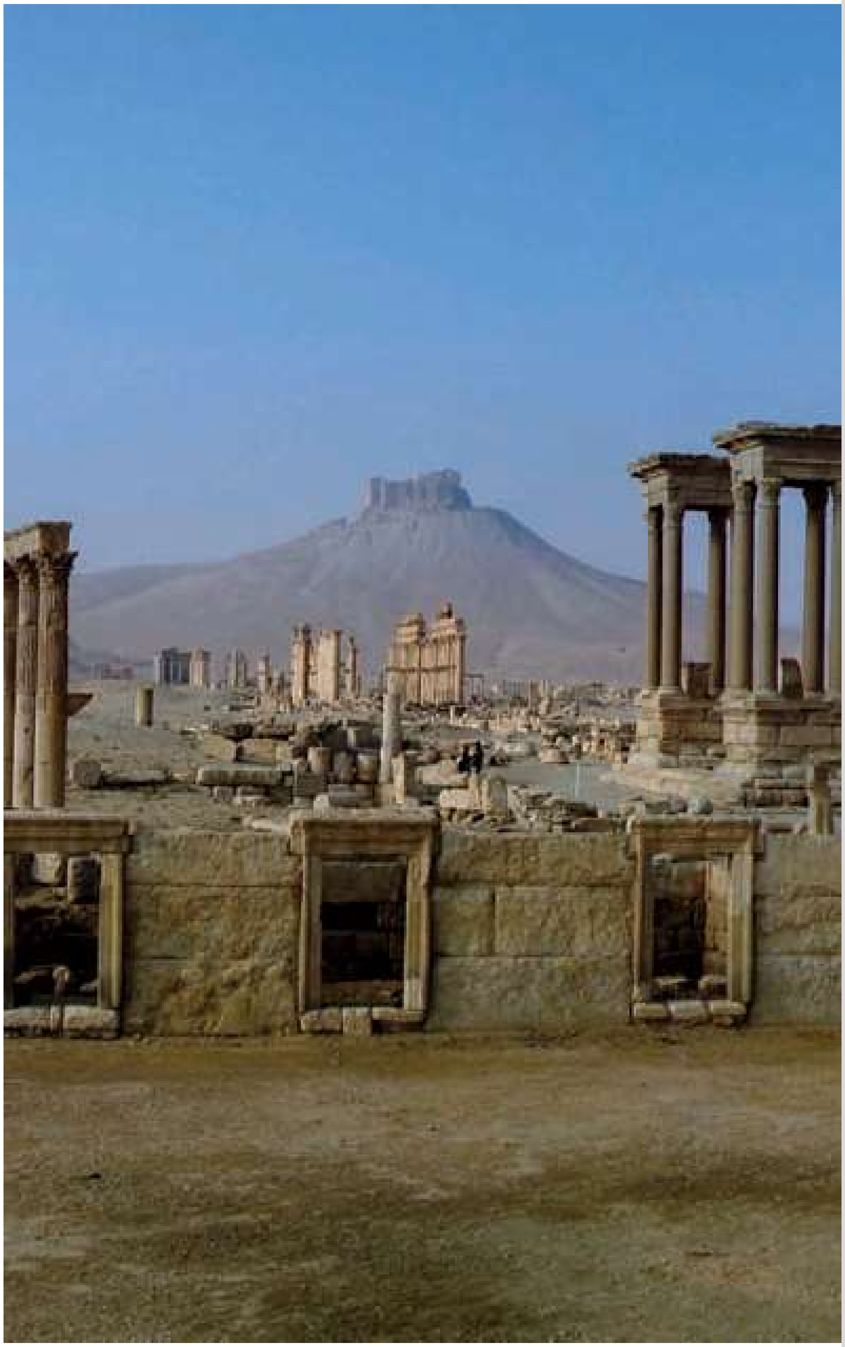
The safeguard of the human's heritage is not just the defense of cultural properties and works of art and thought.
Technological development and empowering role of IT has enabled the creation of information and images silos, such as copies of originals, to guarantee the memory and the accessibility of the assets over time and place. In some cases, the digital copy is the only copy that survived to the destruction of the original one.
Humanity's cultural heritage is under attack for economic interests or new iconoclastic phenomena. It is not to be undervalued the risk that the attacks to the integrity and availability should extend to digitals' copies, to completely alienate the memory of the target cultural heritage.
You notice how increasingly concrete the dual use of cyber attacks is. Methods already practiced to public entities can effectively be used towards warehouses or silos of cultural information. These attacks are increasingly executed with hybrid techniques whose response passes through preparation, identification, mitigation, technical and perhaps political answers.
Regard computerized cultural heritage increasingly as a critical resource, like critical infrastructures, to be protected from targeted threats aimed to alteration or radical alienation. Engineers' skills and defense's techniques play a key role in the organizational and technical response to these threats.
The goal is Right-To-Be-Remembered (RTBR) instead of Right-To-Be-Forgotten (RTBF) as from GDPR.

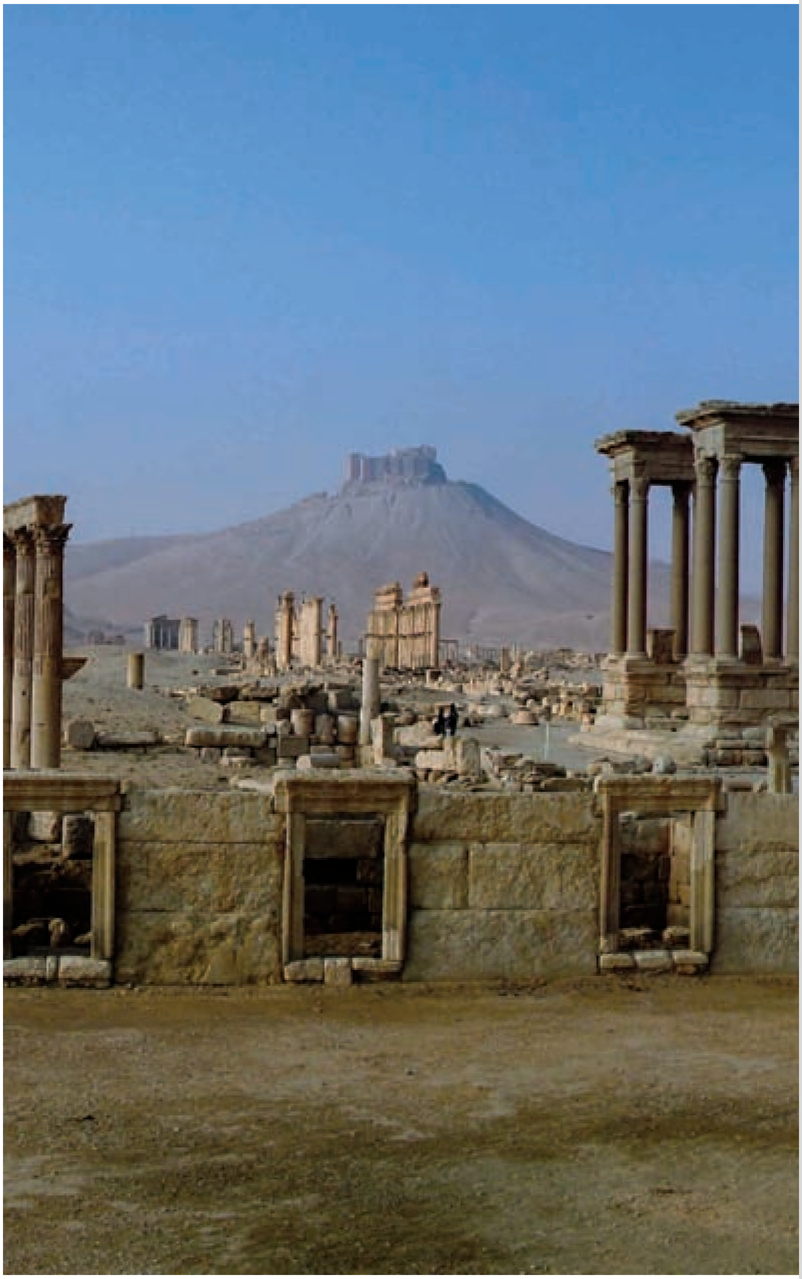


a cura di **ING. G. G. ZORZINO**[1], **ING. A. PRAITANO**[1], **ING. M. PIRRÒ**[2]

[1] Cybersecurity commission, Ordine degli Ingegneri di Roma, Italy
[2] Ordine degli Ingegneri di Napoli, Italy

andrea.praitano@gmail.com
giuseppe.zorzino@mclink.it
pirro.mariano@gmail.com

The safeguard of the human's heritage is not just the defense of cultural properties and works of art and thought.
Technological development and empowering role of IT has enabled the creation of information and images silos, such as copies of originals, to guarantee the memory and the accessibility of the assets over time and place. In some cases, the digital copy is the only copy that survived to the destruction of the original one.
Humanity's cultural heritage is under attack for economic interests or new iconoclastic phenomena. It is not to be undervalued the risk that the attacks to the integrity and availability should extend to digitals' copies, to completely alienate the memory of the target cultural heritage.
You notice how increasingly concrete the dual use of cyber attacks is. Methods already practiced to public entities can effectively be used towards warehouses or silos of cultural information. These attacks are increasingly executed with hybrid techniques whose response passes through preparation, identification, mitigation, technical and perhaps political answers.
Regard computerized cultural heritage increasingly as a critical resource, like critical infrastructures, to be protected from targeted threats aimed to alteration or radical alienation. Engineers' skills and defense's techniques play a key role in the organizational and technical response to these threats.
The goal is Right-To-Be-Remembered (RTBR) instead of Right-To-Be-Forgotten (RTBF) as from GDPR.



a cura di **ING. G. G. ZORZINO**[1], **ING. A. PRAITANO**[1], **ING. M. PIRRÒ**[2]

[1] Cybersecurity commission, Ordine degli Ingegneri di Roma, Italy
[2] Ordine degli Ingegneri di Napoli, Italy

andrea.praitano@gmail.com
giuseppe.zorzino@mclink.it
pirro.mariano@gmail.com

HYBRID CYBER THREATS TO HUMANITY'S CULTURAL HERITAGE: RISKS AND OPPORTUNITIES

MY DESKTOP BACKGROUND

TABLE OF CONTENTS

HYBRID THREATS

Hybrid is the new "buzzword" in the military field

Exploitation of vulnerabilities on the target, using conventional and unconventional methods, to generate ambiguity to hinder decision-making processes

- ✓ generate surprise;
- ✓ seize the initiative;
- ✓ generate deception and ambiguity;
- ✓ avoid attribution of action;
- ✓ maximize deniability of responsibility for aggressive actions.

The resulting mixture of Cyberspace with other enablers like Air and Space domains, the so-called "cyber dimension of Hybrid Warfare", could represent a risk to national interests, cultural too.

Dual perspectives for the use of cyberspace:

- *as an attack on warfare domain*
- *as an threat on assets, goods, economy, culture, infrastructure, human psychology, etc.*

How they work

"Multimodal, low intensity, kinetic and non-kinetic threats to international peace and security including cyber war, low intensity asymmetric conflict scenarios, global terrorism, piracy, transnational organised crime, demographic challenges, resources security, retrenchment from globalization and the proliferation of weapons of mass destruction were identified by NATO as so called hybrid threats"[1]

There is a variety of hybrid cyber threats:

- cyber espionage by State actors for economic and intelligence objectives;
- cyber hacking through individual and organized actors, organized crime (involved in narcotics, arms, human, illicit trafficking in antiquities or works of art, and other threats);
- attacks on Integrity, and Availability domains of security (C.I.A.);
- …

[1] "BI-SC Input to a New NATO Capstone Concept for the Military Contribution to Countering Hybrid Threats." 2010. http://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

ICONOCLASTIC ATTACKS

Iconoclastic attacks to cultural heritage sites are:

- on the historical or archaeological heritage of a nation,
- often originated by a true or supposed iconoclastic justification,
- motivated by religious or politically non-conforming prescriptions.

The last most sensational cases of targeted destruction of cultural goods have taken place in Syria, some of which are also World Heritage Site (UNESCO heritage).

Previously, it had happened in recent time with:

- the library heritage of Timbuctu in Mali for the sake of the Mahdi,
- the Taliban's Bamiyan Buddhas,
- …

Remember the Latin phrase "*damnatio memoriae*".

INFORMATION SILOS OF CULTURAL HERITAGES

Some cultural sites in "List of World Heritage in Danger [1]" have been completely documented (satellites photos, laser scanner 3D detection, images, history, etc.).

Other endangered sites, at the border or near to instability areas around the world, need to be fully documented.

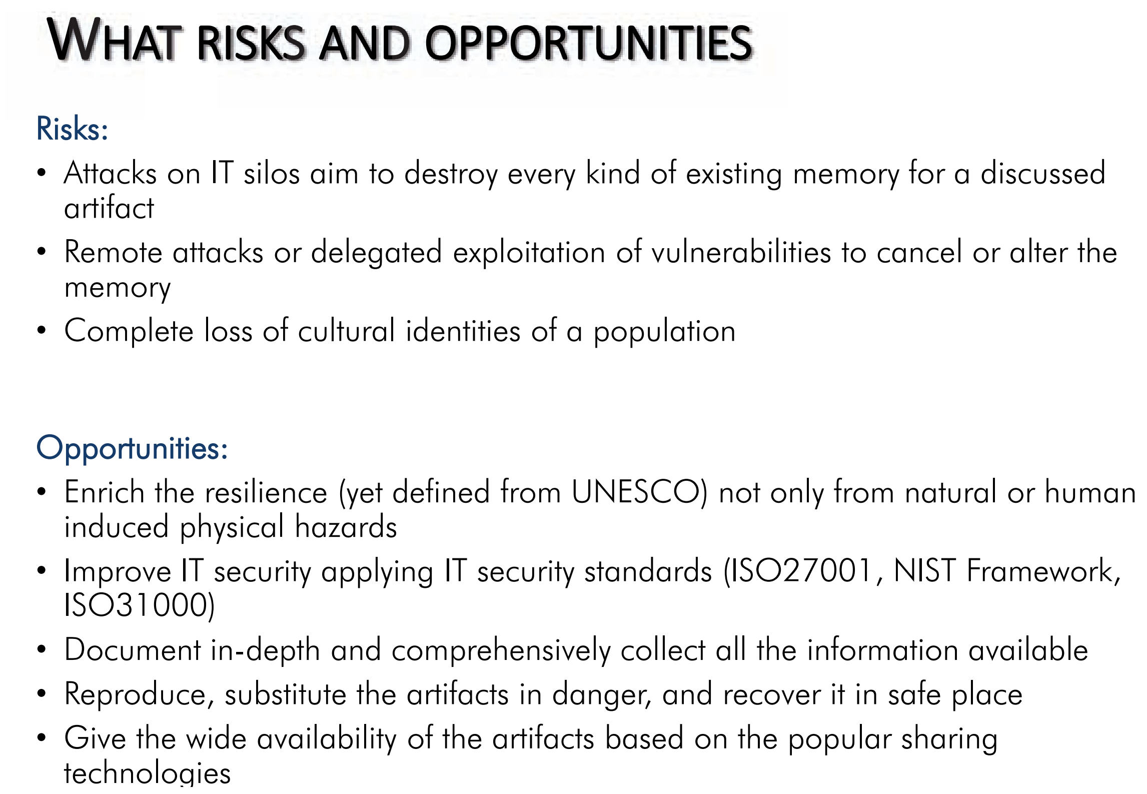
All this info must to be maintained into information silos of cultural patrimony to preserve the cultural heritage and forward it to future generation.

This IT sites or IT silos need:

- to be protected (IT secured)
- to be promoted to UNESCO Cultural Heritage Sites like the artifacts they document because they are "the last repositories of cultural identities of a population"

[1] http://whc.unesco.org/en/158/

4



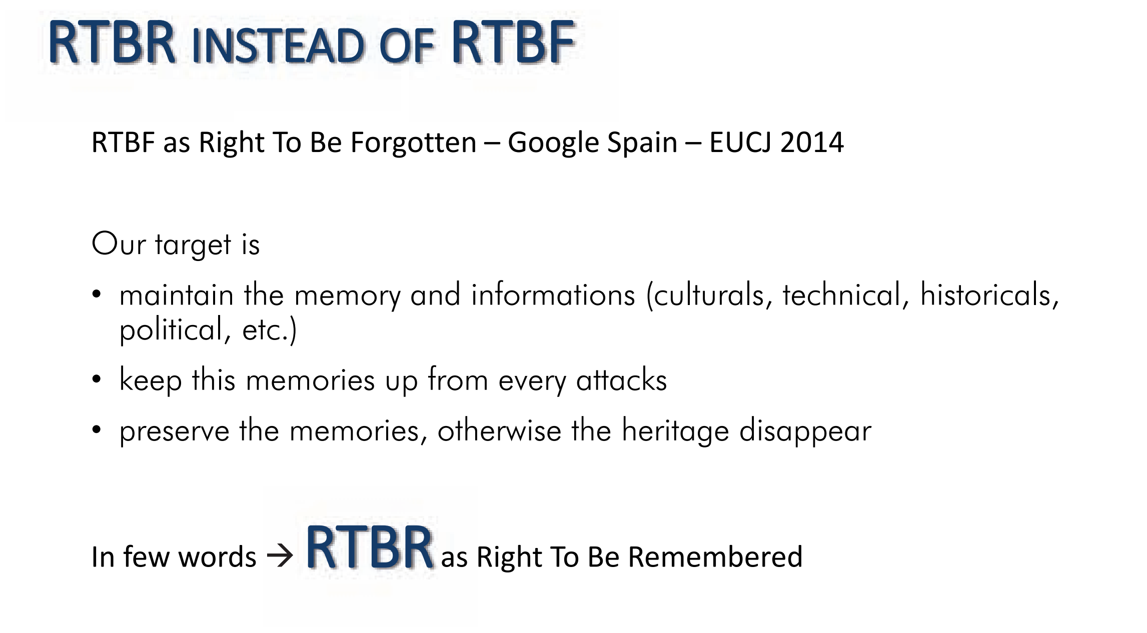
What risks and opportunities

Risks:

- Attacks on IT silos aim to destroy every kind of existing memory for a discussed artifact
- Remote attacks or delegated exploitation of vulnerabilities to cancel or alter the memory
- Complete loss of cultural identities of a population

Opportunities:

- Enrich the resilience (yet defined from UNESCO) not only from natural or human induced physical hazards
- Improve IT security applying IT security standards (ISO27001, NIST Framework, ISO31000)
- Document in-depth and comprehensively collect all the information available
- Reproduce, substitute the artifacts in danger, and recover it in safe place
- Give the wide availability of the artifacts based on the popular sharing technologies



RTBR instead of RTBF

RTBF as Right To Be Forgotten – Google Spain – EUCJ 2014

Our target is

- maintain the memory and informations (culturals, technical, historicals, political, etc.)
- keep this memories up from every attacks
- preserve the memories, otherwise the heritage disappear

In few words → **RTBR** as Right To Be Remembered

WAY AHEAD

- Digital heritage transformation as a way to protect the “original” sites based on a digitalisation standard
- IT silos → gain the status of UNESCO sites of cultural heritage mainly for destroyed site(s) the digital version became the “primary” site
- Activate all IT strategies (security governance) to protect the integrity and availability of documentation data of UNESCO
- Aware the people to hinder the potential threats to alter the information describing the cultural assests
- A new way to make available the digitized cultural heritage of the artifacts

The target is

"Right To Be Remembered" or RTBR

Right To Be Forgotten
DENIED
RTBF