Information Security in Classified Environments

Thierry Laurent - 2019

Contents

- Introduction
- Why Discussing Classified Environments?
- What is a Classified Environment?
- Classification Scales
- Security Clearance
- Access Control Challenge
- Main Issues
- How to Secure?
- Conclusions

Introduction: Who am I?

Thierry Laurent

- IT : one of my favourite hobbies since… the 1979 Apple II!
- Studied IT but university background in social sciences & economy
- Researcher for four years in UCL
- 24 years in IT with more than 20 full years in Information security & BCM
- Owns ProtICT since 2016

Introduction: Who am I?

Why Infosec in “Classified Environments”?

- Got my first NATO secret security clearance in 1985
- More than 10 years of experience in “classified” (military/law enforcement/civilian) environments

Introduction: General Disclaimer

"Classified" means Confidentiality!

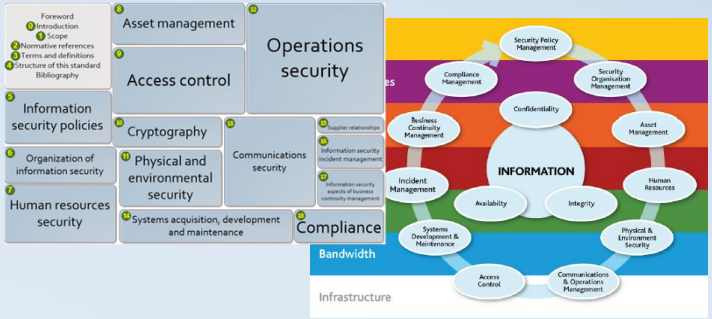
CONTENTS WILL FOCUS ONLY ON:

- outdated specific or published examples
- no link with specific locations or organizations
- no information about current security measures

Why Discussing Classified Environments?

- Exemplary cases of formal/legal boundaries

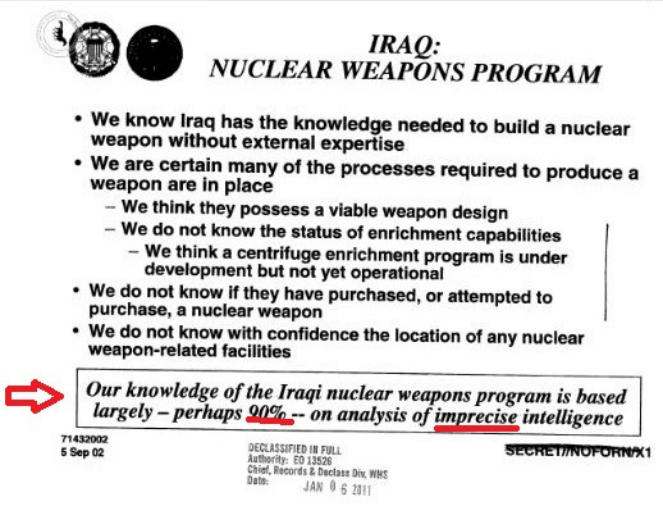
- Combine all dimensions of information security

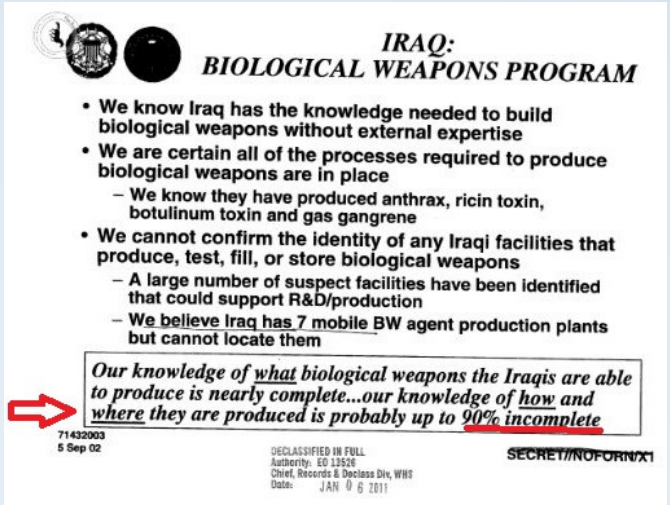


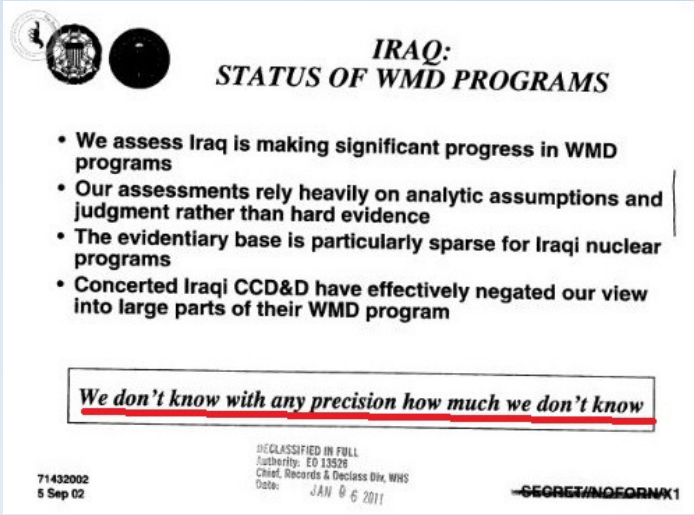
- A glimpse into what may be the future of cybersecurity
  - classified environments: first cyberwar targets!

Why Discussing Classified Environments?

- Illustrates contemporary questions:
  - Legal protection of the state … or secrecy of illegitimate political practices…?







Why Discussing Classified Environments?

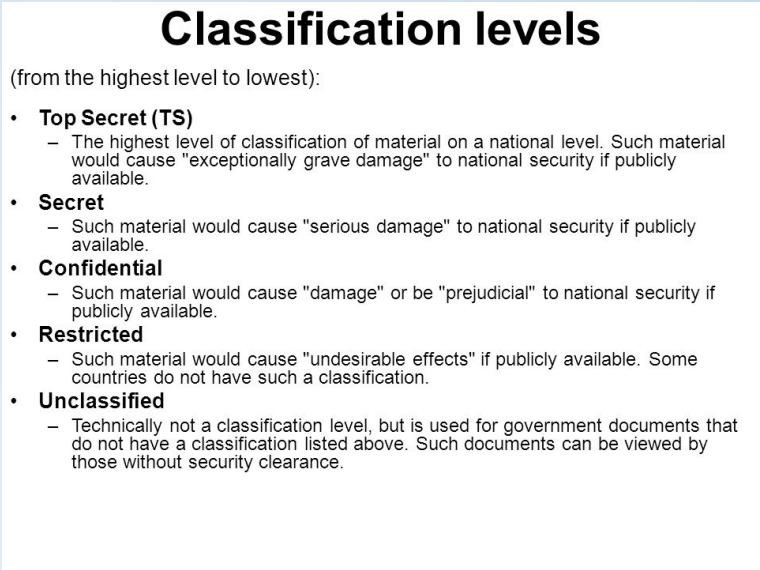
- Illustrates contemporary questions:
  - Activity of whistle-blowers defending privacy and democratic rights

WikiLeaks **vs.** CENTRAL INTELLIGENCE AGENCY

What is a Classified Environment?

Main goal: preserve confidentiality of classified assets (information assets directly linked to the security/sovereignty of a National State or an Entity made of a group of States)

- Complies formally with legal norms rather than "business"-driven ones.
- Relies on a formal "standard" security scale that is national impact ("damage")-driven in Western countries.



Classification levels

(from the highest level to lowest):

- **Top Secret (TS)**
  - The highest level of classification of material on a national level. Such material would cause "exceptionally grave damage" to national security if publicly available.
- **Secret**
  - Such material would cause "serious damage" to national security if publicly available.
- **Confidential**
  - Such material would cause "damage" or be "prejudicial" to national security if publicly available.
- **Restricted**
  - Such material would cause "undesirable effects" if publicly available. Some countries do not have such a classification.
- **Unclassified**
  - Technically not a classification level, but is used for government documents that do not have a classification listed above. Such documents can be viewed by those without security clearance.

What is a Classified Environment?

Mainly public bodies:

- Military headquarters & premises,
- Governmental crisis centres,
- Foreign affairs and defence ministries,
- Intelligence, security and law enforcement agencies,
- Security operations centres for sensitive ICT infrastructure,
- International organisations sites (e.g. NATO-SHAPE)

What is a Classified Environment?

Sensitive civilian premises / critical infrastructures:

- Data centers
- Nuclear & scientific labs
- etc

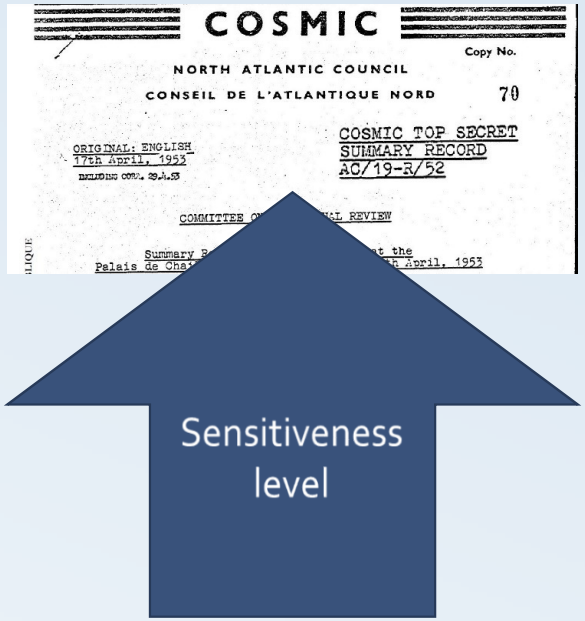
What is a Classified Environment?

AND private subcontractors!

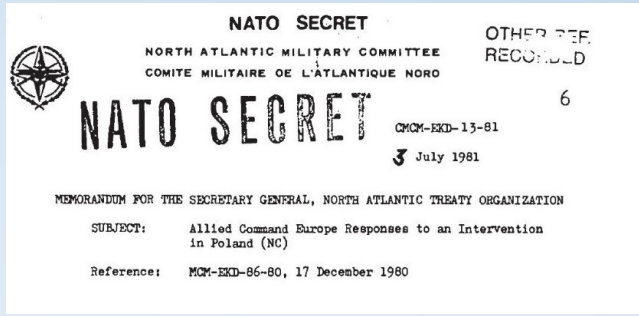
- Military industry,
- Air & space,
- Energy,
- Engineering,
- Enforcement & security,
- ICT,
- Biotechnologies,
- etc.

Classification Scales

Various flavours: National – NATO – EU



- Top secret – Cosmic Top secret
- Top secret – Focal Top secret
- Secret - Atomal
- Confidential
- Restricted
- Limited High
- Limited Basic – Official Use Only – Unclassified but Sensitive
- Public - Unclassified


NATO SECRET

NORTH ATLANTIC MILITARY COMMITTEE
COMITE MILITAIRE DE L'ATLANTIQUE NORD

NATO SECRET

CMCM-EKD-13-81

3 July 1981

MEMORANDUM FOR THE SECRETARY GENERAL, NORTH ATLANTIC TREATY ORGANIZATION

SUBJECT: Allied Command Europe Responses to an Intervention in Poland (NC)

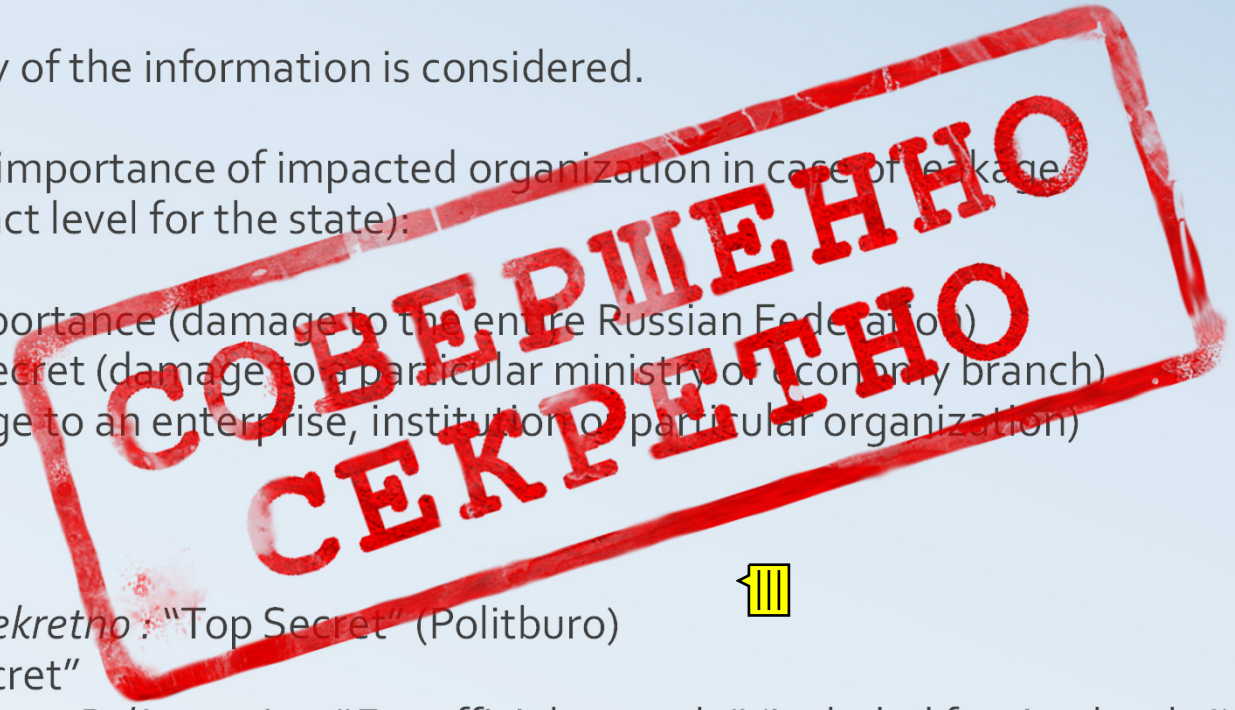
Reference: MCM-EKD-86-80, 17 December 1980

Classification Scales

Russia: Specificity of the information is considered.

Scale is linked to importance of impacted organization in case of leakage (rather than impact level for the state):

- Of Special Importance (damage to the entire Russian Federation)
- Completely Secret (damage to a particular ministry or economy branch)
- Secret (damage to an enterprise, institution or particular organization)



USSR

- *Overshenno Sekretno :* "Top Secret" (Politburo)
- *Sekretno:* "Secret"
- *Dlya Sluzhebnogo Pol'zovaniya:* "For official use only" (included foreign books!)

Classification Scales

Secrecy ?
as old as the first state.
Anything could be "secret" without formal definition.

"Classification" is far more recent: generally formalized during the 20th century.

Laws clarify essentially:

- What shall be AND shall not be classified
- Information classification duration per category (e.g. 30 – 20 – 10 years)
- Standard de-classification and disposal processes

Classification Scales

China:

Laws formalizing defined classification levels were published in…

… 2010 and classification standards in March 2014!

State Secrecy Bureau's March, 2014 Interim Provisions on Management of State Secrets Classification (国家秘密定密管理暂行规定)

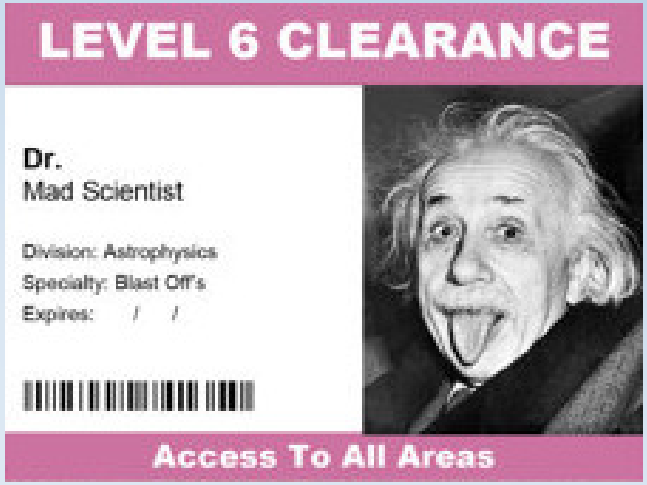
https://chinaspc.files.wordpress.com/2014/12/classification-regulations-translation.pdf

Goal: fight against "red stamping" intended to cover corruption/bribing/etc…

Security Clearance

Classification relies on the Security Clearance principle:

- Status granted to an individual allowing him access to classified information or supporting assets including restricted areas.
- Requires a formal validation by a national state authority after a background check.
- International classification (e.g. NATO or EU) relies on cross-certification of national clearances



Security Clearance

- Company clearance:
  - accounting health,
  - economic status of the company,
  - export activities (sales of sensitive material to sensitive countries),
  - etc.
- Appointment of a company dedicated security officer in charge of security clearances management

Security Clearance

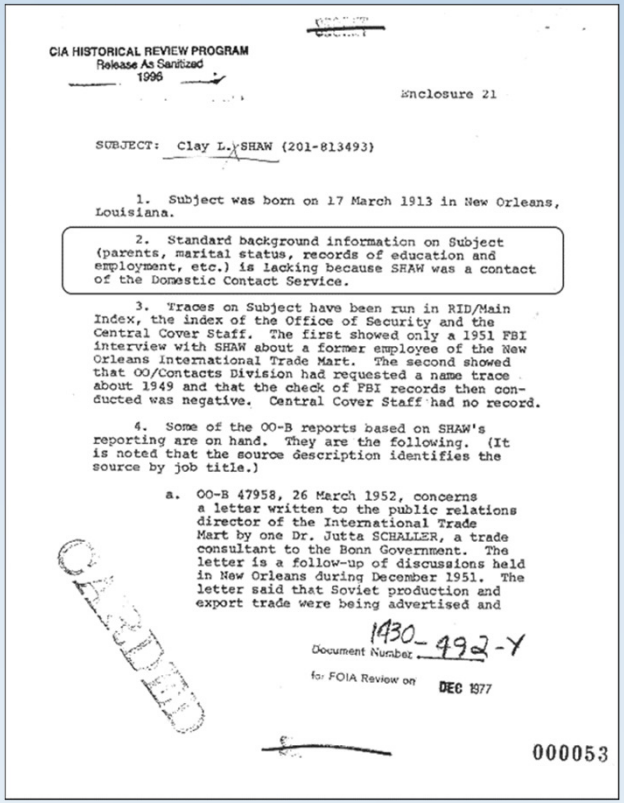
- Personal clearance:
  - criminal record,
  - financial records,
  - prior jobs,
  - political activities,
  - association membership,
  - travels in sensitive countries,
  - etc.

Security Clearance

Complexity and thoroughness of the clearance process depends on the country National Security Authority and the requested level.

Background checks and administrative validation ask for:

2-3 months to … 2 years!



CIA HISTORICAL REVIEW PROGRAM
Release As Sanitized
1996

Enclosure 21

SUBJECT: Clay L. SHAW (201-813493)

1. Subject was born on 17 March 1913 in New Orleans, Louisiana.

2. Standard background information on Subject (parents, marital status, records of education and employment, etc.) is lacking because SHAW was a contact of the Domestic Contact Service.

3. Traces on Subject have been run in RID/Main Index, the index of the Office of Security and the Central Cover Staff. The first showed only a 1951 FBI interview with SHAW about a former employee of the New Orleans International Trade Mart. The second showed that OO/Contacts Division had requested a name trace about 1949 and that the check of FBI records then conducted was negative. Central Cover Staff had no record.

4. Some of the OO-B reports based on SHAW's reporting are on hand. They are the following. (It is noted that the source description identifies the source by job title.)

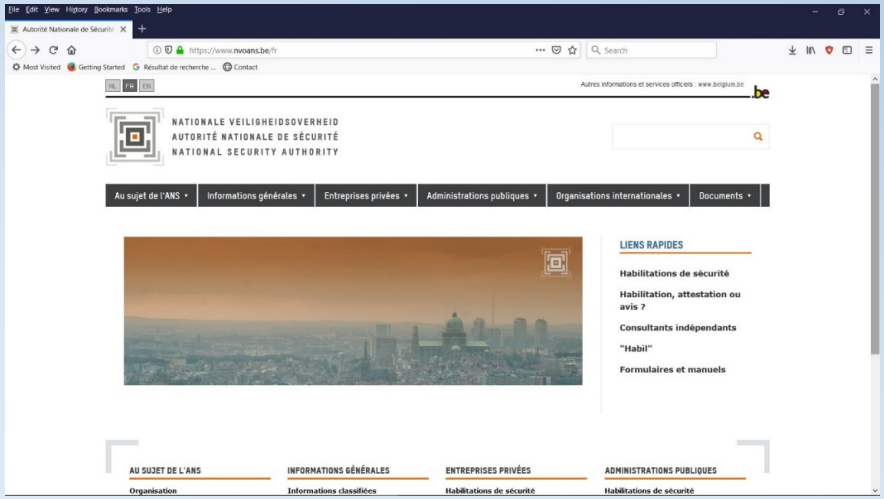
a. OO-B 47958, 26 March 1952, concerns a letter written to the public relations director of the International Trade Mart by one Dr. Jutta SCHALLER, a trade consultant to the Bonn Government. The letter is a follow-up of discussions held in New Orleans during December 1951. The letter said that Soviet production and export trade were being advertised and

CANCELLED

Document Number 1430-492-Y
for FOIA Review on DEC 1977

000053

Security Clearance



In Belgium:

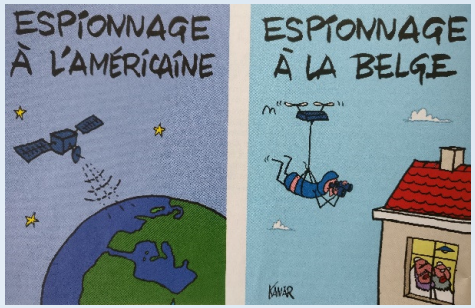
Autorité Nationale de Sécurité

www.nvoans.be

Relying on:

- VVSE ("Sûreté de l'état": 600 FTE)
- SGRS ("Service Général du Renseignement et de la Sécurité": 600 FTE)

Legal basis: https://www.nvoans.be/fr/faq/cadre-legislatif



Security Clearance

- Some figures in Belgium (2016):
  - Delivery of 7452 personal security clearances
  - Delivery of 262 company clearances
  - 862 cases of collaboration with foreign authorities willing to deliver clearances
  - 34.134 security checks (90% to access European summits or critical infrastructures such as airports)
- Number of files is increasing yearly (+10 to 25%) in spite of the fact the cost of the procedure is now heavy (1200€ per company & 2[illegible]0€ per individual for a Secret clearance) whereas some years ago it was…free!

Security Clearance

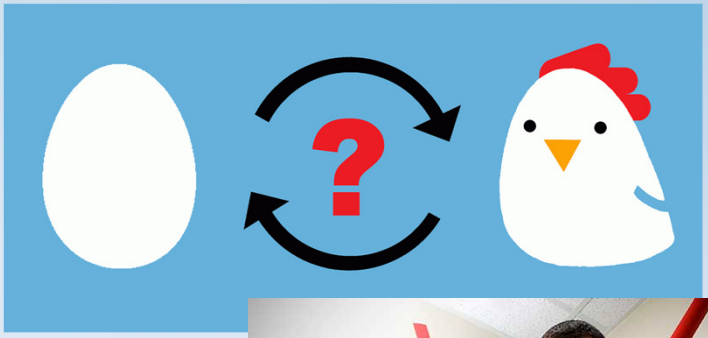
- Personal clearance request issue?

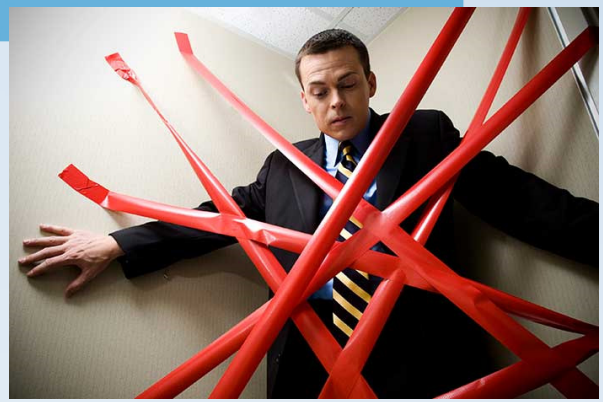
This shall be requested to work on a known project

BUT working on a project processing classified data requires a clearance to get any access… !

Moreover the process is long and cumbersome…

So, many people must start "working" with a request proof and a criminal record evidence or an outdated clearance… ☹





Security Clearance

Access Control Challenge?

Old challenge: close to impossible to map assets/human resources in a large organization.

- Cold war techniques of classified information circulation relied on:
  - Avoid transmission of digital versions
  - Use of human “mules” to transmit critical documents
  - Printing signature techniques
  - Old encrypting techniques such as DES for highly sensitive digital documents
  - Perimeter security for fully isolated ICT systems
  - Limit access to data: “need to know” principle
  - Rely on “four eyes” principle for all critical information processing
  - Log/archive all workflow processes steps implementation

Access Control Challenge?

Some use cases of organisational weaknesses:

- Document archiving
- Document storage
- Document duplication

Access Control challenge?

21st century: Some apparent changes such as:

- Mapping of classified document national central registry and security clearances.
- Reliance on various techniques to individualize documents (e.g. crypto signature).
- Application-controlled lifecycle of most sensitive documents.
- Use of Big data mining-like techniques.

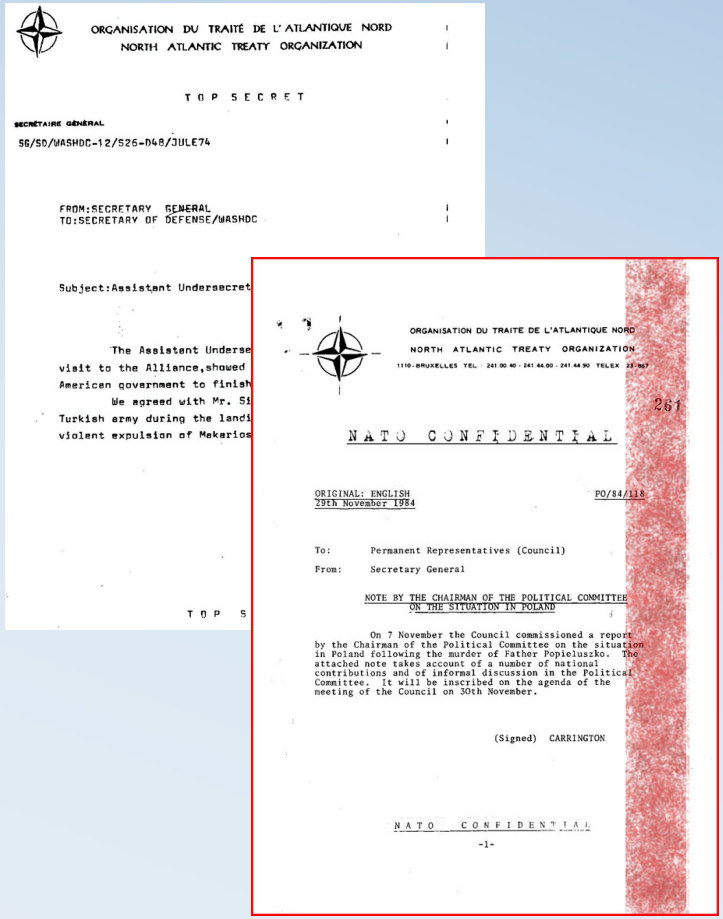
Access Control Challenge?

- Data mining technologies are promising…
  - e.g. to identify valuable human targets! Combination of decisional capability/access to very sensitive information (variety/combination)

But the human factor stays the weakest link…!

And such technologies are expensive for the “weakest link” of a chain

  - E.g. NATO: decentralized national control



ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
NORTH ATLANTIC TREATY ORGANIZATION

TOP SECRET

SECRÉTAIRE GÉNÉRAL

SG/SD/WASHDC-12/526-D48/JULE74

FROM:SECRETARY GENERAL
TO:SECRETARY OF DEFENSE/WASHDC

Subject:Assistant Undersecret

The Assistant Underse
visit to the Alliance,showed
American government to finish
We agreed with Mr. Si
Turkish army during the landi
violent expulsion of Makarios

TOP S

ORGANISATION DU TRAITE DE L'ATLANTIQUE NORD
NORTH ATLANTIC TREATY ORGANIZATION
1110-BRUXELLES TEL. : 241.00.40 - 241.44.00 - 241.44.90 TELEX 2

261

NATO CONFIDENTIAL

ORIGINAL: ENGLISH
29th November 1984

PO/84/118

To: Permanent Representatives (Council)
From: Secretary General

NOTE BY THE CHAIRMAN OF THE POLITICAL COMMITTEE
ON THE SITUATION IN POLAND

On 7 November the Council commissioned a report by the Chairman of the Political Committee on the situation in Poland following the murder of Father Popieluszko. The attached note takes account of a number of national contributions and of informal discussion in the Political Committee. It will be inscribed on the agenda of the meeting of the Council on 30th November.

(Signed) CARRINGTON

NATO CONFIDENTIAL

-1-

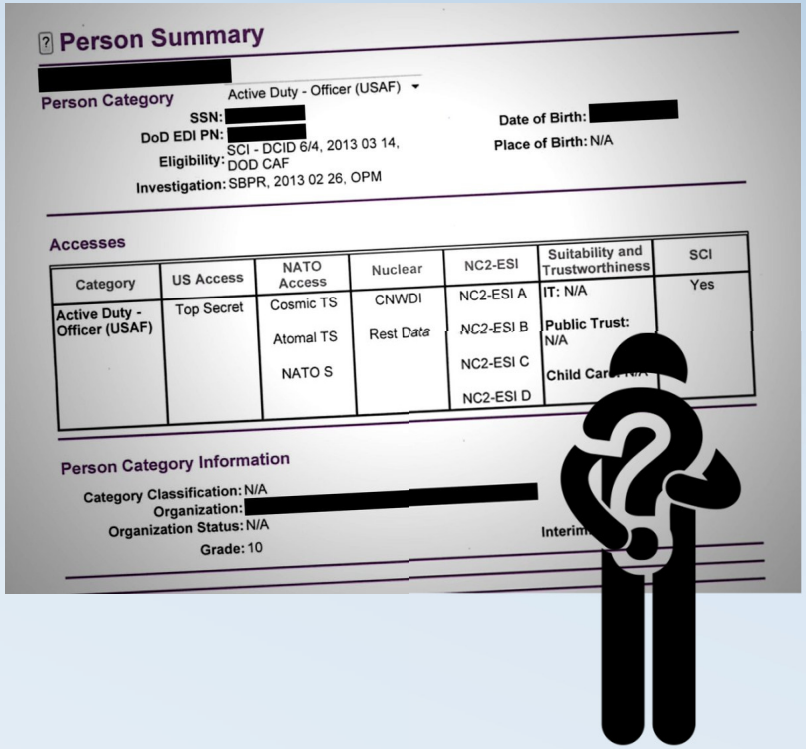
Access Control Challenge?

Better control BUT

… the risk grew noticeably:

- E.g. if 99.9 % of the cleared US citizens comply with the rules…

  …5000 individuals have a non-compliant behaviour (security leakage, espionage, absent-minded loss of classified data, etc.)!

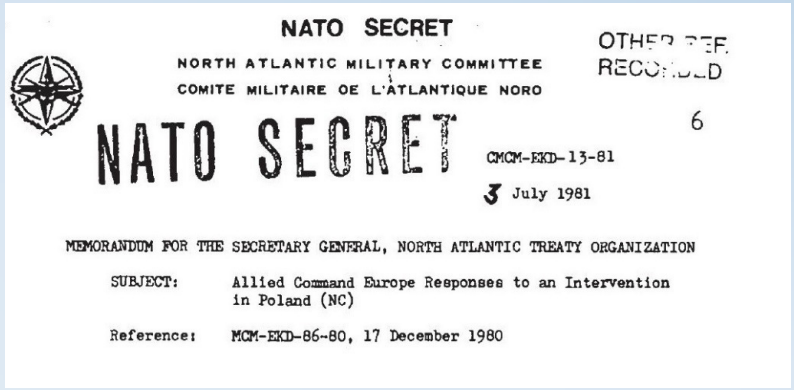


Main Issues

- Classification: self-generating monster!

In spite of pre-defined areas of acceptable classification of information.

Any reference to a classified document theoretically requires the same level of classification!



NATO SECRET

NORTH ATLANTIC MILITARY COMMITTEE
COMITE MILITAIRE DE L'ATLANTIQUE NORD

OTHER REF. RECORD

6

NATO SECRET

CMCM-EKD-13-81

3 July 1981

MEMORANDUM FOR THE SECRETARY GENERAL, NORTH ATLANTIC TREATY ORGANIZATION

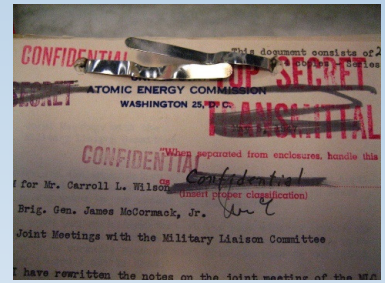
SUBJECT: Allied Command Europe Responses to an Intervention in Poland (NC)

Reference: MCM-EKD-86-80, 17 December 1980

E.g. Sensitive topic (Secret)
-> Meeting organisation to discuss the topic (Secret)
-> Decision to cancel the meeting (Secret)!

Main Issues

- Mislabelling of classified information



- Public bodies frightened by the classification requirements weight

This opens a paradox: a very sensitive environment is sometimes not formally classified and rely on third-party classification (e.g. international/mutualized environments)

Main Issues

- Subcontractors control: who needs a clearance?

It is not uncommon that hundreds of people in a large subcontracting company get partial access to data related to a sensitive project.

  - E.g. The European parliament questions regarding the Orange leakage concerning TESTA-based information
  - E.g. Rumours of F-35 technical data Chinese hack

Main Issues

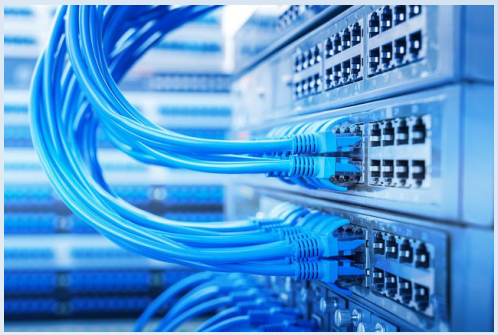
Security technologies:

- Lack of specific “reliable” security systems?
- Use of Russian, Israeli, US or Chinese technologies… Alternatives???

Main Issues

- Isolation of networks is becoming a BIG issue
  - Network interconnection for quick communication purposes
  - Very high complexity of networks and inability to get fool proof environments (technology vulnerability/compatibility/maturity issues)
  - Interconnection of networks with different levels of trust/security for resilience purposes (e.g. SDnetwork)
  - Network interconnection legacy issue (e.g. security level change)
  - Network security heterogeneity (e.g. weakest link in continental networks covering various countries, multiple topologies, various technologies, etc.)

Arpanet



Main Issues

- Prevention of unauthorized access is becoming a BIG issue:
  - Cost of risk prevention related to mobile connectivity
  - The “lost” USB stick syndrome
    - The US military headquarters data theft by the PLA unit 61398
    - The Stuxnet case (US/Israeli attacks against the Iranian nuclear program)
  - Risk prevention related to BYOD
    - e.g. scanners to detect mobile/smart phones/smart devices

There are solutions but most are:

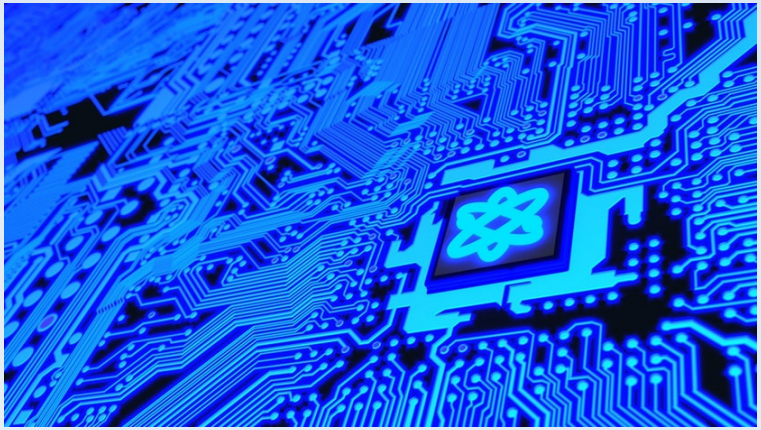
VERY expensive

Only reliable in highly controlled environments

Very efficient in limited scale infrastructures

Main Issues

We can fortunately rely on encryption on vulnerable network segments or to protect sensitive storage… BUT



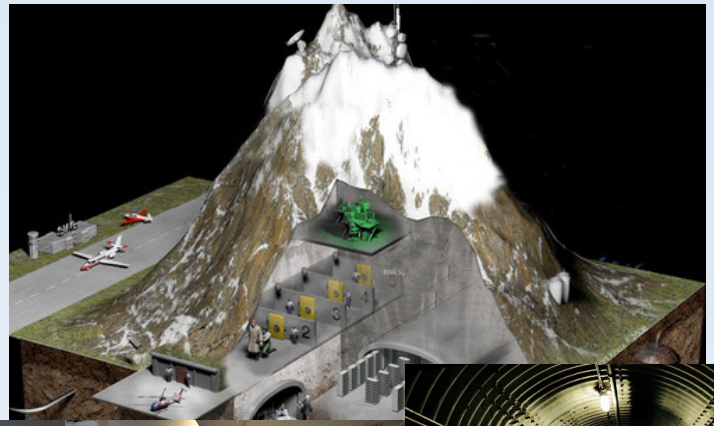
Obsolescence of standard cryptographic algorithms such as AES is foreseen for… +/- 2025 - 2030 at the latest!

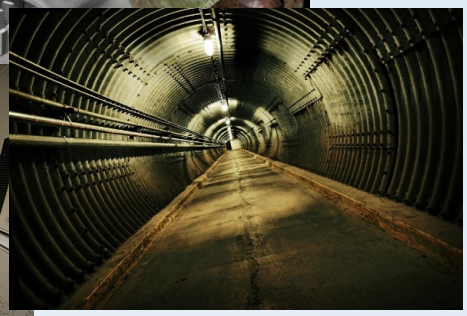
The culprit: Quantum computing cyberwar capabilities…

Is this one of the reasons behind the Chinese “Great Firewall” and the Russian disconnected Internet?

Main Issues

- The infrastructure cost & management issue





The "James Bond" base

vs the "temporary" solutions... ☹

Main Issues

- The infrastructure cost & management issue
  - Long-term strategic vision questions
  - Lack of security awareness from politicians and civil servants

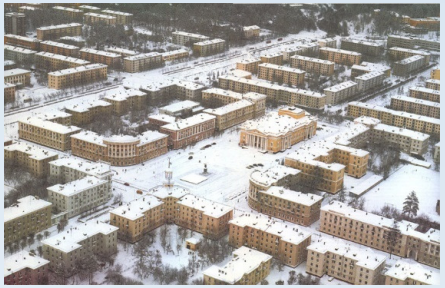
Main Issues

- The infrastructure cost & management issue
  - Lack of available budgets
  - Length of time to build “hard” infrastructures

Cold War classified environment extreme examples: full cities!


Mercury (US)


Tomsk-7 (USSR)


Krasnoiarsk-26 (USSR)


City 404 (China)

Main Issues

- The Democratic control:

The most sensitive state secrets are

sometimes…

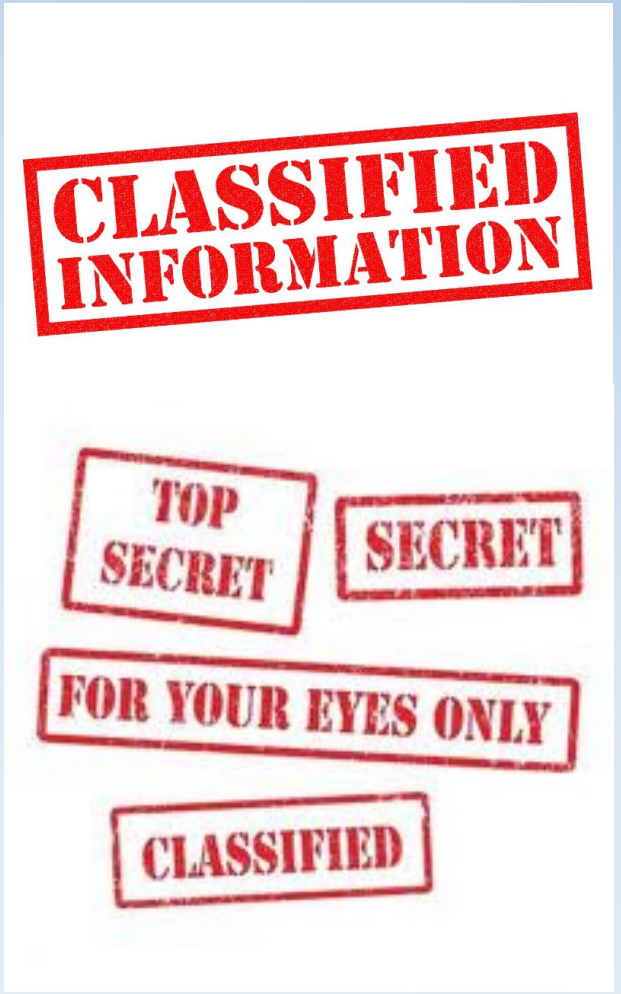
Not classified!…

  - e.g. the Umicore role in the atomic bomb race & military nuclear programs.

How to Secure?

How do you build your security measures?

- Classification formal security requirements
- Specific legal basis
- Risk analysis (methodology & tool)



How to Secure?

Classification frameworks are just one source of security requirements…

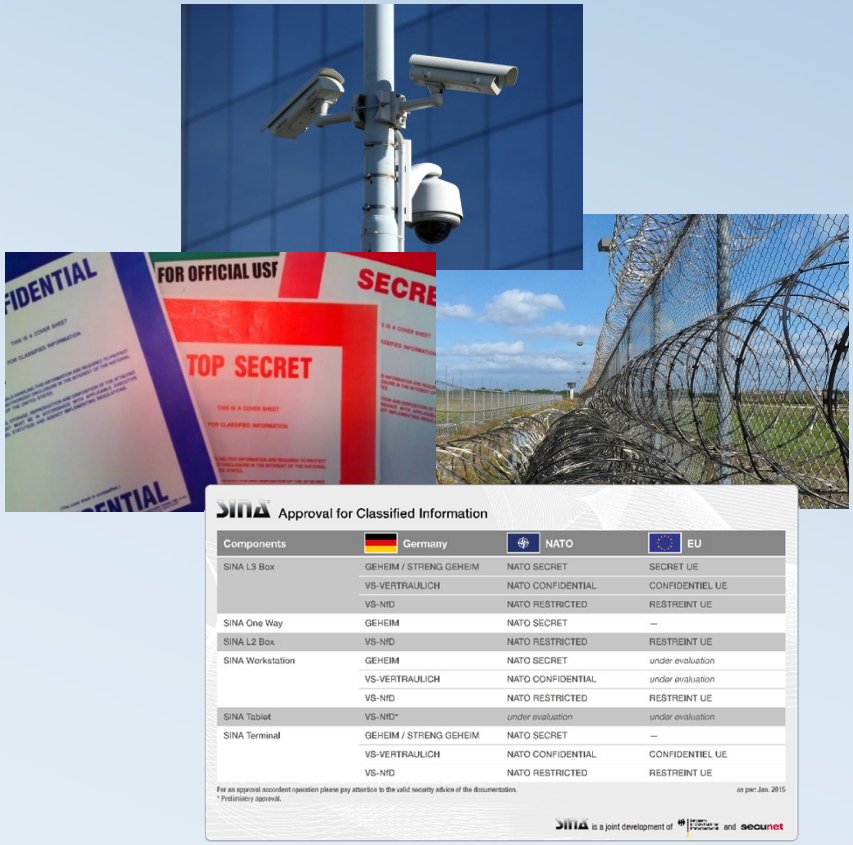
BUT when you build security requirements for one environment that needs to be security cleared, classification regulations have always the top priority, before considering other legal regulations, sectorial norms, risk-based management standards, best practices and so on!

How to Secure?

Practically:

- Physically isolated areas with individual access and multi-layer security systems (fences, guards, CCTVs, badge-controlled access with PIN /biometrics information, intrusion detection systems, etc.)
- Network segregation & defence in depth (“air gap” - cryptos – firewalls – IDS – application proxies – etc.)
- Single use of physical IT assets, full ownership (no “cloud”) & system hardening
- Tight control on information lifecycle: creation – processing – duplication – communication – storage – disposal
- Formal trainings regarding clearance impact and security awareness
- Strong access control: Need to know – 4eyes – SoD
- Encryption at all levels (authentication, signature, storage, timestamping, etc.)
- Physical access control rules for external parties
- Formal IT (service) management rules (ITIL-like)
- Etc.

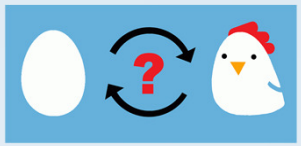
V E R Y H E A V Y !



How to Secure?

Problem: information is classified but not physical assets as such!

BUT obtaining an ICT environment that is compatible with classification rules asks for years…



One solution: comply with classification rules for a formally non-classified environment to be ready
BUT this has a heavy cost.

How to Secure?

Formal risk analysis tools such as CRAMM or EBIOS

Theory
Standard and formalized approach
Comprehensive database
Used as a permanent tool to support an ISMS cycle

CRAMM

Practice
Incredibly cumbersome and time consuming (>expensive)
Database not regularly updated
Rarely if ever used on an ongoing basis
Ask for a LOT of manual fine-tuning • To link assets to countermeasures • To update contents • To overcome the rigid approach

For experienced people: still more efficient to rely on the methodology but use a “manual” approach!

How to Secure?

In practice:

- Comply strictly with legal and classification regulations
- Clarify the business requirements sensitiveness but stay reasonably on the “safe side”
- In case of doubt, never underestimate the risk
- Rely on norms and risk analysis tools as safeguards but not as final solutions
- “Trust no one” when you build the rules: the human factor stays the weakest link
- Adapt later the rules to the reality of the environment (up or down in a PDCA cycle perspective)
- Financing cannot be a major problem

Final Question: the Risk

- Data leaks, espionage, cyberwar, etc.

Aren't we exaggerating the risk…?

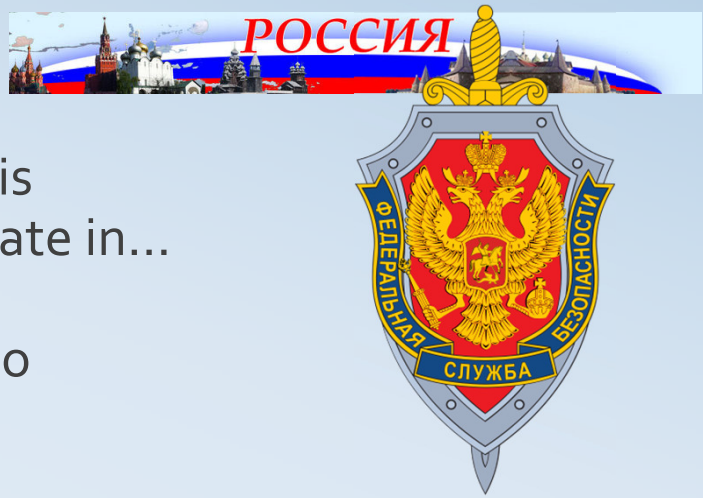
Well… NO!!!

Final Question: the Risk

The “Red colonel” case (1988)

Final Question: the Risk

April 2018: The "Pol Grégoire" scandal.

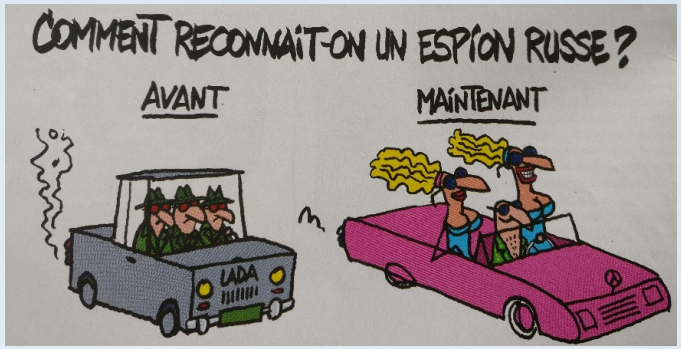


Foreign affair diplomat working for the KGB since 1987. His activities were seemingly discovered by the Security of State in… 2012 whereas he was still active!
He delivered documents, Belgian ID cards and passports to Russian undercover agents.
Conclusion: 6.271€ of fine and 1 year of suspended prison sentence!

Final Question: the Risk

Today: probably between 250 & 300 Russian & Chinese agents in Belgium.
(Service Européen Action Extérieure)

April 2019: the Serbian-Russian connection: in 2016, one SGRS major would have disclosed confidential information to a Serbian lady working probably for the Russian FSB. Current conclusion: the deputy director resigned…



Final Question: the Risk

And what about our "partners/allies"?
The Juste Lipse wiretapping case (French, German & Spanish EU Council delegations) (1995-2003)

Final Question: the Risk

The Belgacom hacking case "Operation Socialist" (2013)

belgacom

?

Conclusions: the Time vs Cost Issue

Classification is just one formalization of the eternal weapon race between the shield and the sword.

All actors are in a world of uncertainties but this is even more critical for the EU because of:

- Increased dependency on digitalization
- New technical challenges (e.g. Quantum)
- Explosion of cost of security technologies able to cope with threats
- Lack of “EU champions”
- Increased uncertainties about alliances in and out of EU

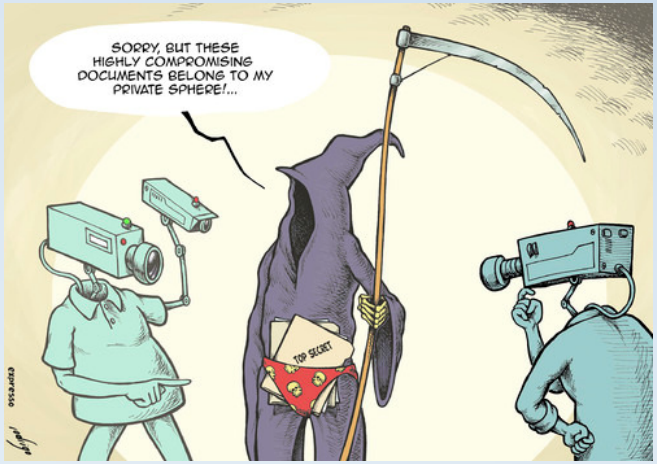
No way to avoid huge investments in the nearby future if EU wants to stay a major actor in the future…

Conclusions: the Human Side

The behavioural aspect: think twice before working in such an environment!

 PLUS	MINUS 
Access to challenging technologies	Not technologically trendy
Full security scope	Cumbersome and rigid processes
Large budgets	Not easy for imaginative or creative mindsets
Access to sensitive security topics	Need to comply with secrecy

Thanks for your attention!



All the pictures used in the document are available on the Internet.

They are only used hereabove for educational illustration purposes.

Please do not re-use them out of such a fair use context without the approval of the owners.

Thanks.