GSAW2015

A SPACE MISSION CYBER-SECURITY STUDY

CODE: GMV-GSAW2015-PRE-001
DATE: 03/03/2015
VERSION: 1

Secure e-Solutions®
GMV SOLUCIONES GLOBALES INTERNET S.A.U.

GMV-UNCLASSIFIED

The information contained within this document is considered as “GMV-Unclassified”. The receiver of this information is allowed to use and redistribute the information, referring the source of the information; observing legal regulations in intellectual property, personal data protection and other legal requirements when applicable.

© 2015 by GMV
Published by The Aerospace Corporation with permission.

gmv® INNOVATING SOLUTIONS

CONTEXT

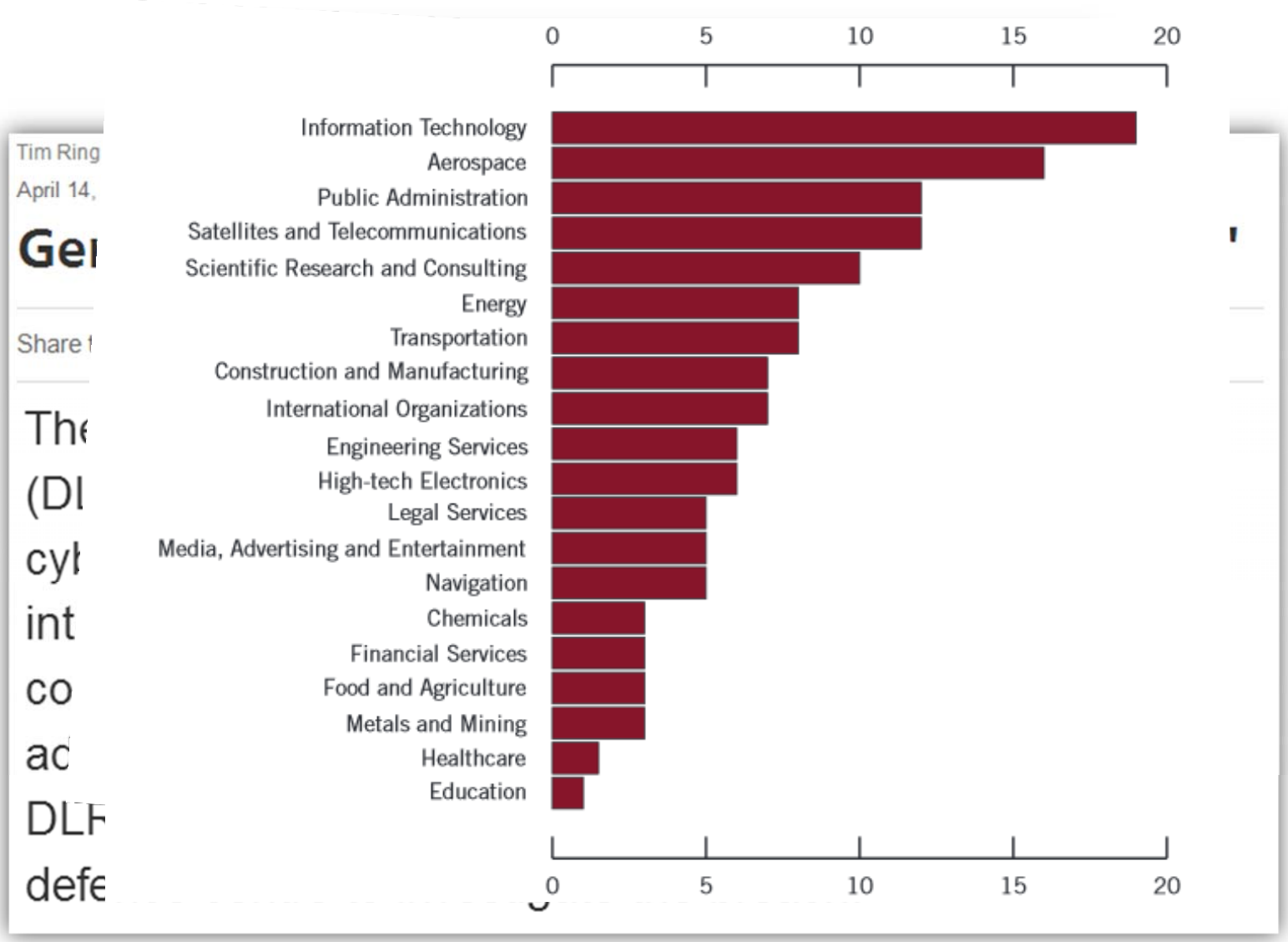
INNOVATING SOLUTIONS

TRENDS

Criticality of space-based services

Battlefield: Cyber-space

AND IN SPACE?


0
5
10
15
20
Information Technology
Aerospace
Public Administration
Satellites and Telecommunications
Scientific Research and Consulting
Energy
Transportation
Construction and Manufacturing
International Organizations
Engineering Services
High-tech Electronics
Legal Services
Media, Advertising and Entertainment
Navigation
Chemicals
Financial Services
Food and Agriculture
Metals and Mining
Healthcare
Education
0
5
10
15
20

SUMMARISING II

BUT… IT ISN'T EASY AT ALL

- Several deeply specialised fields converge
- Very complex systems
- Large infrastructures
- Lots of actors
- Dependencies, interconnections,…

PROPOSAL

GMV-UNCLASSIFIED

INNOVATING SOLUTIONS

REQUIREMENTS

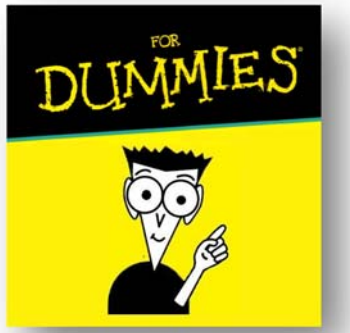
- SIMPLICITY & USABILITY: TOOL SUPPORT
- FLEXIBILITY AND ADAPTABILITY
- COMPLETE
- EASY TO MAINTAIN AND EVOLVE
- INTERNAL CROWDSOURCING
- HOMOGENIZE
- FULL OWNERSHIP TO ESA

© GMV, 2015
GMV-UNCLASSIFIED

SOLUTION CONCEPTS

A PRIORI RISK ASSESSMENT & TREATMENT RECOMMENDATIONS

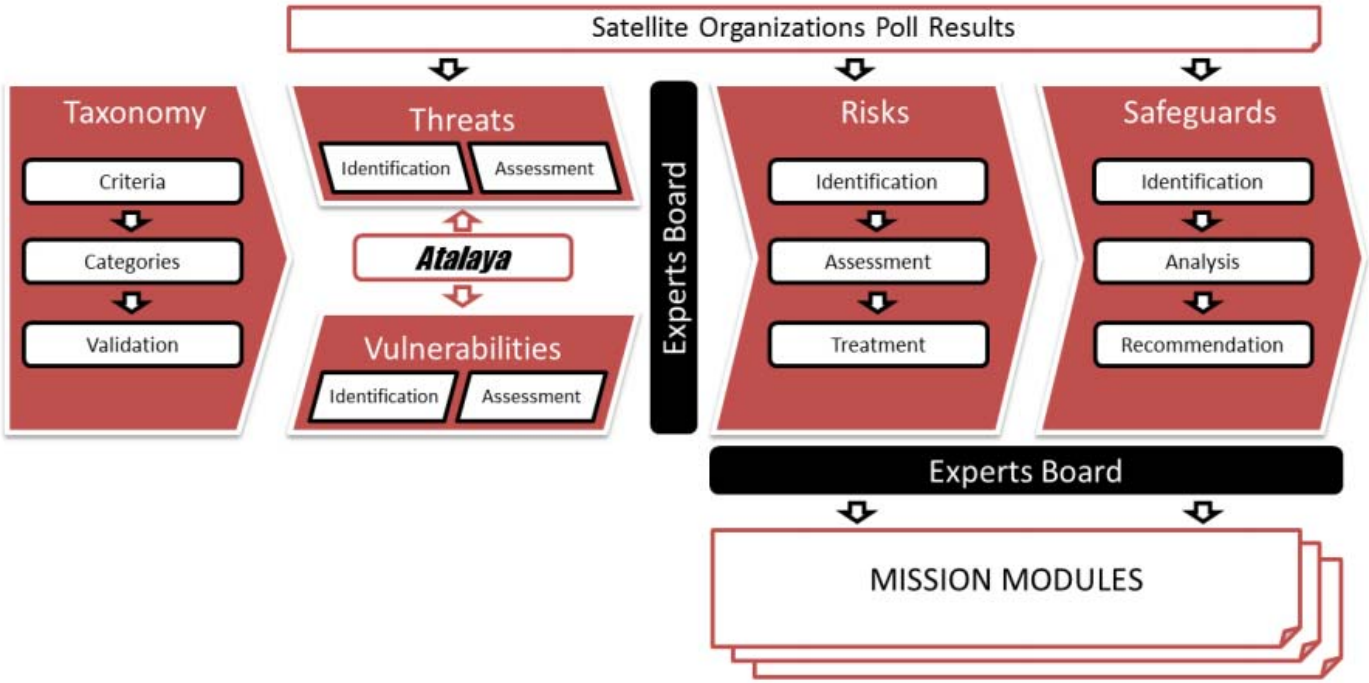
- MODULARITY CONCEPT:
  - EXPLOIT COMMONALITIES
  - ADAPT TO PARTICULARITIES
- FOR DUMMIES AND EXPERTS



METHODOLOGY

INNOVATING SOLUTIONS

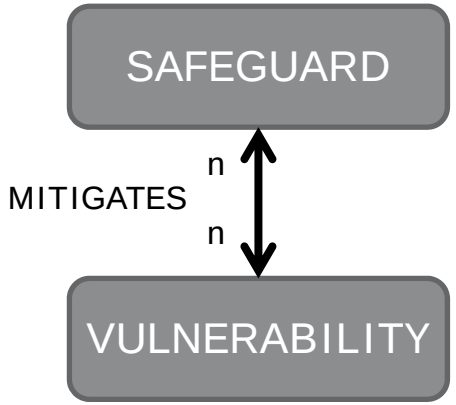
METHODOLOGY



- WE WILL TAKE A RECOMMENDED SAFEGUARD AND GO BACKWARDS

SAFEGUARD

"Event Logging" in phase E of a mission

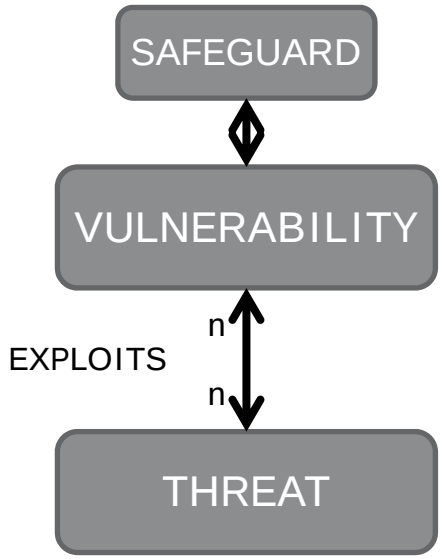


- Can be HIGH or BASIC
- Mitigates vulnerabilities:
  - Directly: removing the vulnerability or the possibility of exploiting it
  - Indirectly: mitigating the consequences of the vulnerability being exploited
- In this case:
  - Untraceability of User Actions
- **BUT**... it is not the only safeguard required to mitigate the vulnerability...

VULNERABILITY

- Is part of a risk (threat-vulnerability pair)
  - It can be exploited by threats
- In our example one threat is:
  - Unauthorized use of rights
- Value based on CVSS:
  - Range
  - Complexity
  - Authentication

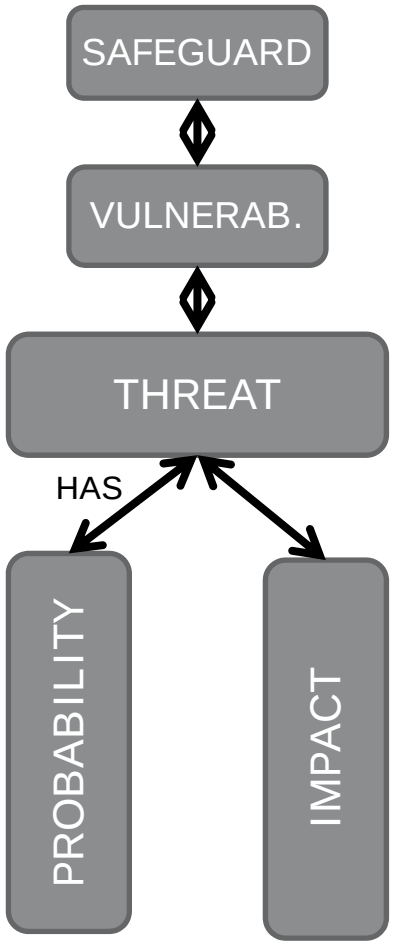
  and
  - Impact



© GMV, 2015
GMV-UNCLASSIFIED

THREAT

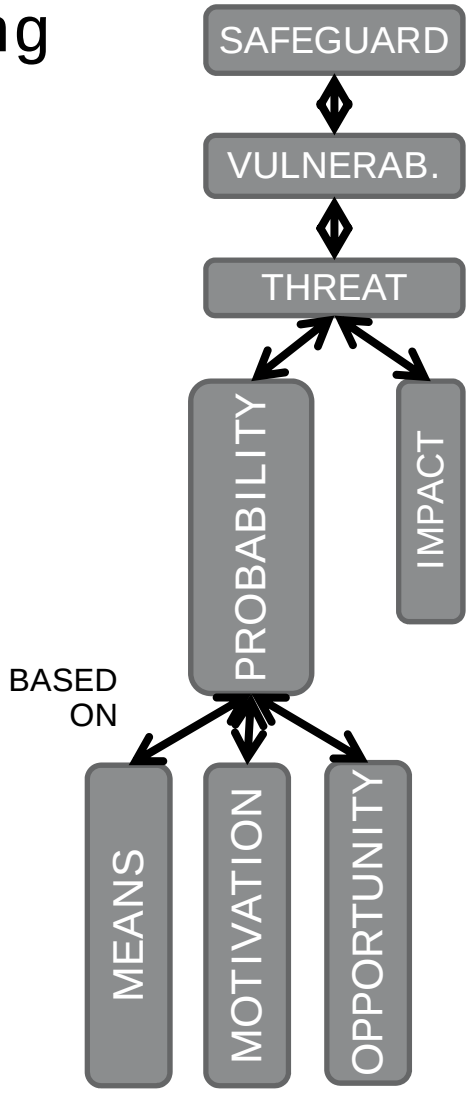
- The risk introduced by a threat is:
  - The Probability of the threat materializing, per,
  - The Impact that it would have if it materializes



© GMV, 2015
GMV-UNCLASSIFIED

THREAT - PROBABILITY

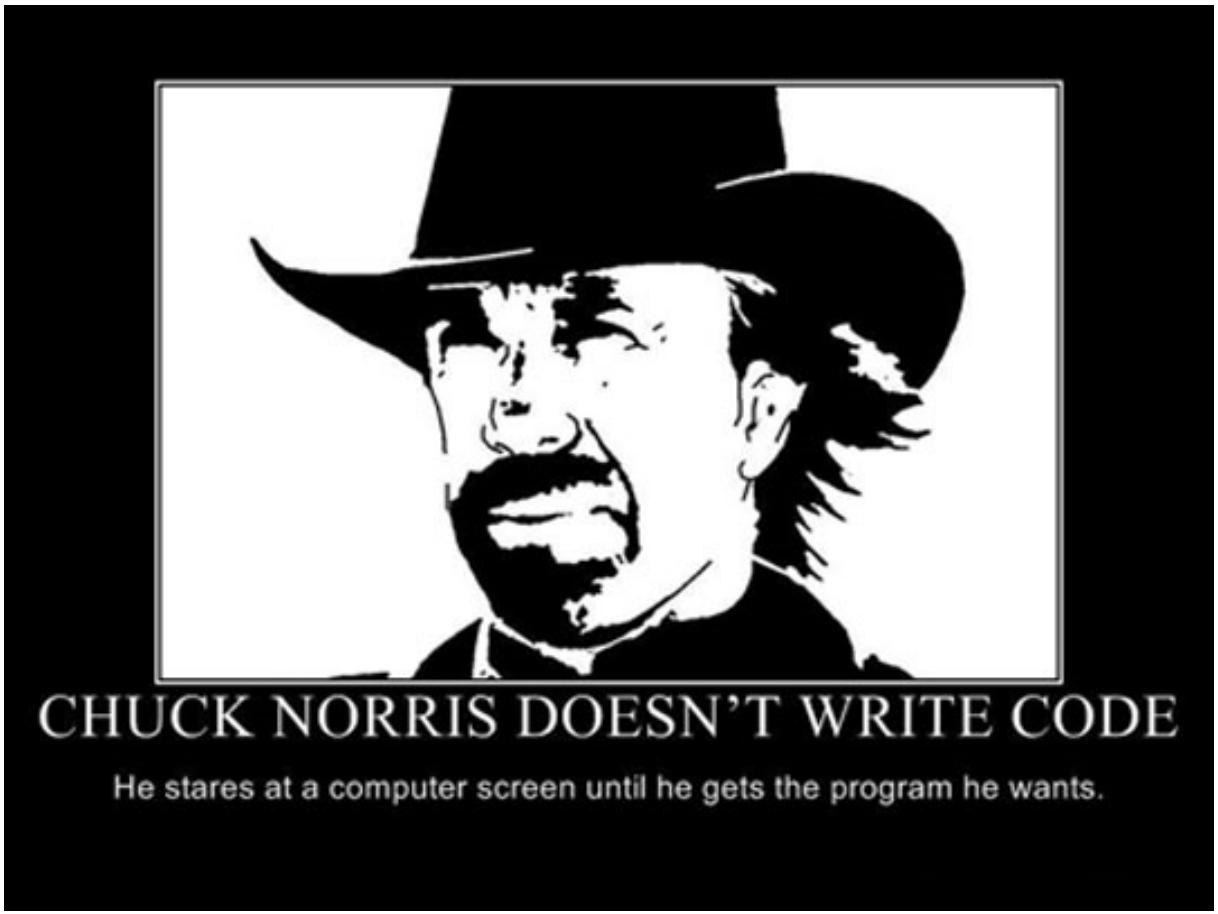
- The probability of a threat materializing depends on the attacker:
  - Means
  - Motivation
  - Opportunity

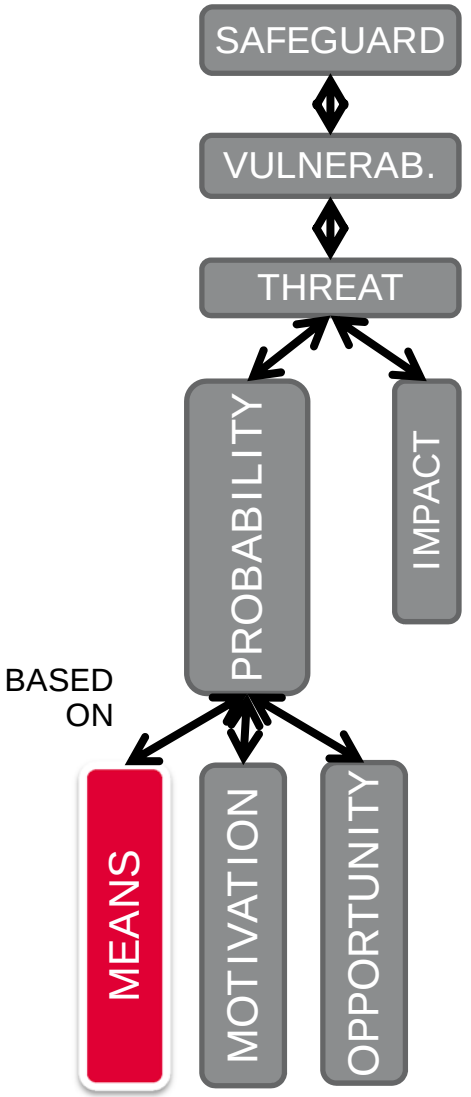


© GMV, 2015
GMV-UNCLASSIFIED

THREAT – PROBABILITY - MEANS

- Linked with the attacker skills and resources

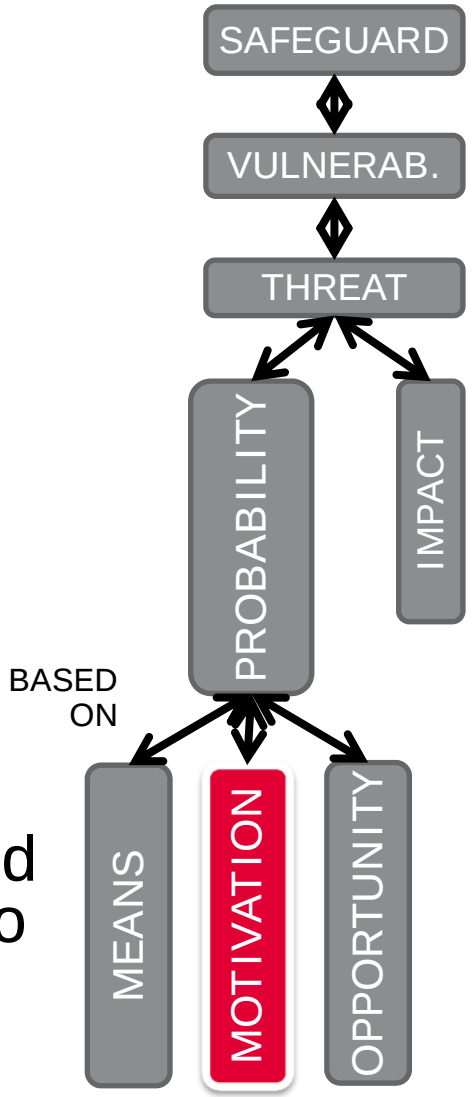




© GMV, 2015
GMV-UNCLASSIFIED

THREAT – PROBABILITY - MOTIVATION

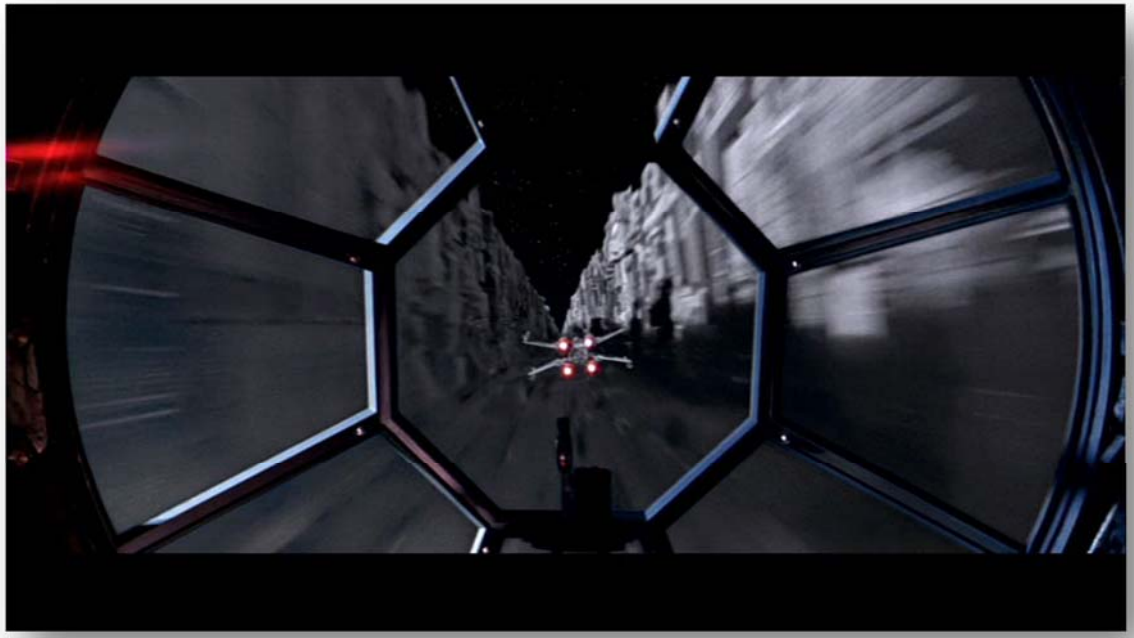
- Linked with the attacker interests and the mission capacities

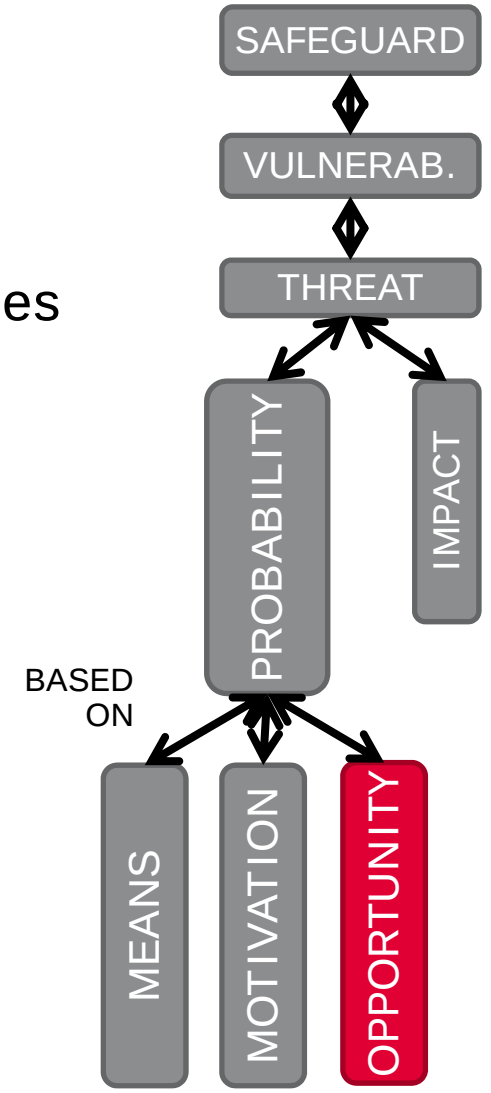


For each mission type we have identified groups of attackers, their motivations to attack the mission and the means.

THREAT – PROBABILITY - OPPORTUNITY

- Based on the existence of vulnerabilities which can be exploited by the threat
  - Takes the MAX of all exploitable opportunities





© GMV, 2015
GMV-UNCLASSIFIED

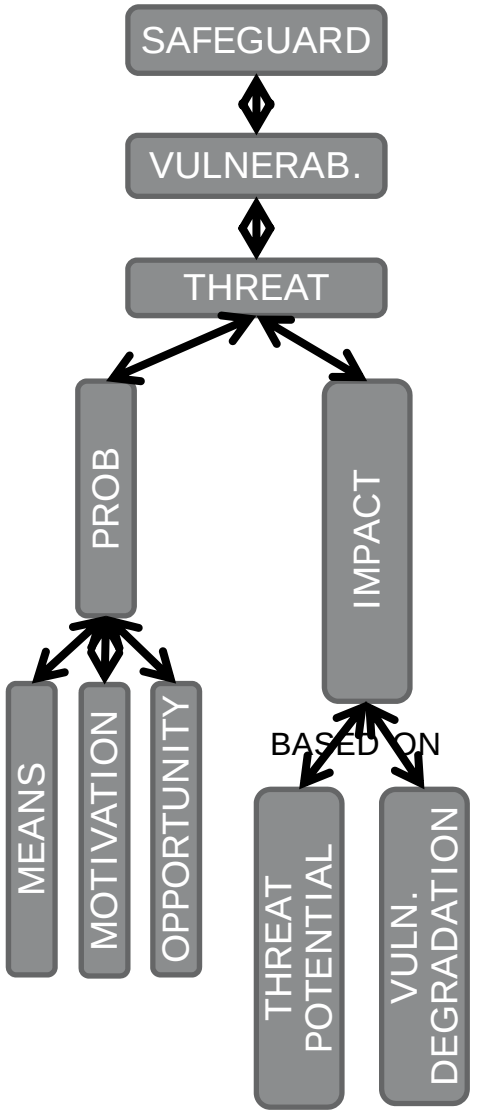
THREAT – IMPACT

- Combines:
  - The threat potential damage

with

  - The degradation allowed by the vulnerability (TOTAL, PARTIAL, NONE)

- Potential damage:
  - Considers the value of each security dimension for the mission
  - Calculated based on impact table



THREAT – IMPACT

	Economic Loss (% of budget)	Impact to image/reputation	Legal impact	Impact to Strategic Position	Impact to society
L1	0,1%	Impact to internal image (unsatisfied, unmotivated employees)	Violation of regulations and laws by an employee, but with no legal impact to organization.	Loss of data with strategic value.	Knowledge development
L2	1%	Impact to technical leadership	Violations of regulations and laws with minor consequences. Minor breaches of contract which result in at most minor contractual penalties.	Strategic service accessible by the enemy.	Impact to non-critical services
L3	10%	Impact to public opinion (utility of mission)	Violations of regulations and laws with substantial consequences. Major breaches of contract with high contractual penalties.	Strategic service degraded. Data with strategic value corrupted.	Critical services degradation
L4	100%	Impact to customers	Fundamental violations of regulations and laws. Breaches of contract with ruinous damage liabilities.	Temporal loss of strategic service.	Critical services unavailability
L5	>100%	Impact to financial credibility of ORG, financial partners relationship	Revocation of the license for space services.	Loss of strategic service.	Safety of life

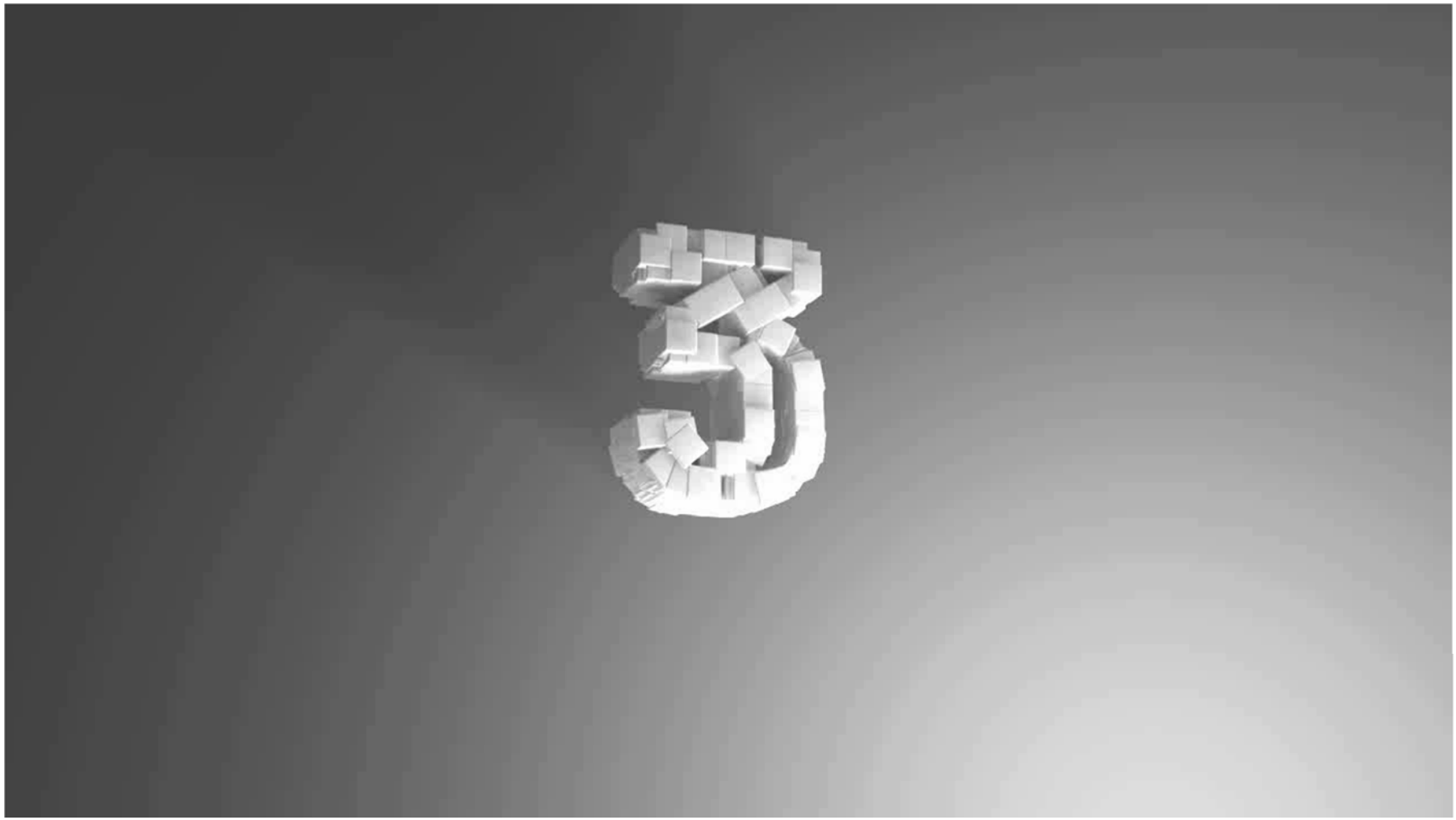
RECAPITULATING

- Launcher missions:
  - Potentially interesting for different attackers for several reasons
  - Some of them might be motivated and have the means to, among many others, execute an “unauthorised use of rights”
  - This threat can exploit “untraceability of user actions”.
  - This has a probability which is a combination of Means/Motivation/Opportunity
  - The Impact which depends on the potential damage and the degradation allowed by the vulnerability for each dimension.
  - The Risk is Threat x Vulnerability
  - To reduce that risk we can apply several safeguards among which “Event Logging”

RESULTS

INNOVATING SOLUTIONS

VIDEO SUMMARY



© GMV, 2015
GMV-CONFIDENTIAL

Thank You

Ricardo Marín
Senior Security Consultant
Email: rmarin@gmv.com
www.gmv.com

gmv®
INNOVATING SOLUTIONS