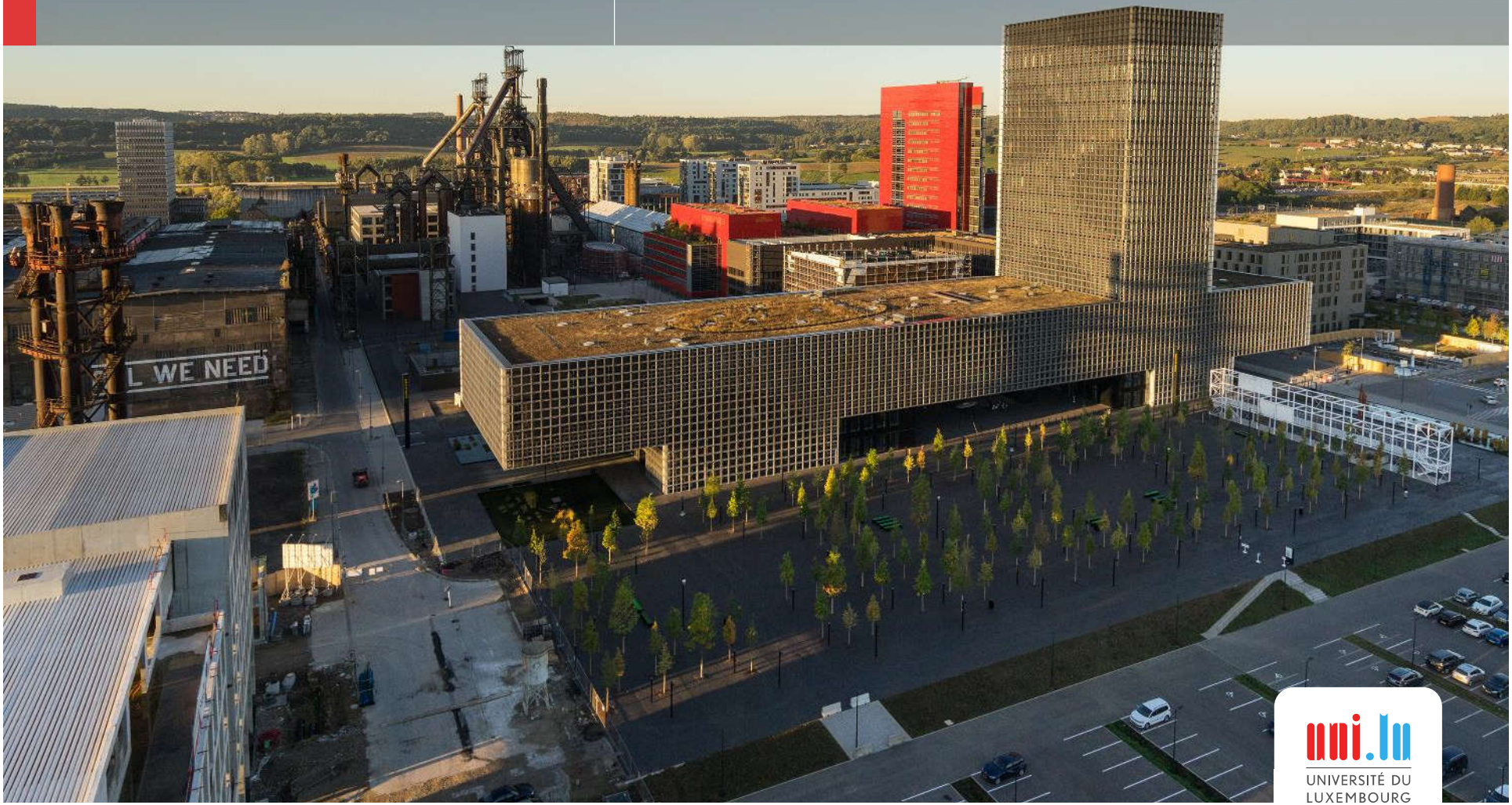
University of Luxembourg

Multilingual. Personalised. Connected.

Space Traffic Management & Cybersecurity

PJ Blount



UNIVERSITÉ DU LUXEMBOURG

- The views expressed do not represent the views of my employer
- **My research is made possible by a generous grant from the Luxembourg National Research Fund.**

Space Traffic Management

Space Traffic Management

- Some legal observations
  - Underlying purpose of space law is to ensure the “maintenance of international peace and security”
  - OST puts emphasis on International Cooperation and Communication as a means to ensure safety and security in space
  - These are soft obligations that frame the underlying ethic of the treaty
    - Free Access for All
  - Space Law calls for a balancing of Strategic, Civil, and Commercial interests in the exploration and USE of outer space

Space Traffic Management

- The problem
  - Increasing amount of space debris
  - Smallsats
  - Very large constellations
  - New space actors
    - States
    - Corporations
    - NGOs
    - Universities
  - No formal system of coordination of space activities
    - Outside of GEO

- Current state of play
  - Major space farers collect and use their own SSA
  - The United States has formal SSA sharing system and distributes Conjunction Data Messages (CDM) to ALL operators
    - This is a military system and high-quality data is classified
    - Modelling and data are not verifiable
  - Other states keep SSA data secret (but share with allies)
  - Commercial solutions have evolved
    - SDA
    - ExoAnalytics

Space Traffic Management is a critical to protecting security of space and commercial investment in space!!!

- A hypothetical:
  - Corporation X in state A receives a CDM for a collision with a nonmaneuverable satellite launched by a university in state B
  - Corporation X's satellite is near end of life and maneuvering it is costly, Corporation X makes the decision not to move satellite and hope for the best

  - Who can compel Corporation X to engage in collision avoidance? Who is a risk? Who is at fault in the case of a collision happening?

Space Traffic Management

- Space Traffic Management
  - Set of legal *and* technical tools needed to ensure security, safety, and sustainability of on orbit activities through the management of space activities
    - Implies authority
  - Space Traffic Coordination?

What's needed?

- Standards
  - Data
  - Modelling
  - Regulatory structures
- What else?
  - TRUST

- Trust
  - By states – national security concerns
    - Trust in system
    - Trust in each other
  - By stakeholders
    - Protection of investments
    - Avoiding regulatory burden
    - Decisions made are proper

- Standards
  - Foster trust through transparency
  - i.e. if a stakeholder can verify the data and the modeling and understand how decisions a processed and made, then the stakeholder will have more trust in the system
  - Standards set norms of behavior that give stakeholder's the ability to identify fault when accidents happen

Space Traffic Management

- Standards
  - Data
    - Need for standardized data for inclusion in multi-sourced data pool
  - Modelling
    - Transparent algorithms that provide for accurate modelling of the space environment
  - Regulatory Framework
    - Regulation, rules, norms, best practices that define responsible space activities
    - Investors want to know about legal risk

Space Traffic Management

- Establishing normal/responsible behavior is critical to commercial operations
  - Space law was established to create trust among space faring nations through cooperation and coordination
  - The problem of STM is the exact type of problem that the OST envisioned
    - Collective action for the benefit and interests of all states by building trust through cooperation, communication, and transparency
- Normalized behavior can be understood as peaceful and can reduce the risk of conflict
  - Example: US-USSR Code of Conduct for naval activities
- Normalized behavior fosters commercial activity by standardizing interactions among market participants

Space Traffic Management

- The space environment is currently being taxed by an increase of users
- STM is critical to ensuring the long-term sustainability of space activities
- Stakeholders will only engage to the extent that they trust the system to serve the interests of the space community (civil, commercial, and military)
- Standardization will be essential to building that trust
- Lack of coordination puts all stakeholders at risk
  - Commercial operators will bear that risk more directly

Coffee Break

Cybersecurity

- What is cybersecurity law?
  - IT DEPENDS!
    - Jurisdiction
    - Type of Data
    - System Specifications (hardware and software)
    - User requirements
- There isn't a universal legal (or technical) standard for the requisite level of cybersecurity
- Cybersecurity is bespoke to each enterprise

- Legal Sources
  - International Law
  - Domestic Legislation
  - Regulations
  - Common law?
  - Contracts

- Non-legal Sources
  - Policy & Strategy
  - Technical Standards
  - Technical Specifications
  - Good practices

Cybersecurity Governance!

- Cybersecurity law is diffuse and it often comes from unexpected places . . .
  - United States: The Federal Trade Commission uses its authority to investigate "unfair and deceptive trade practices" to investigate data breaches (upheld by 3d Circuit)
  - EU: Everybody's favorite – GDPR. It's about keeping PII secure, which implicates your systems
  - Multiple Jurisdictions: Emerging rule that Board has fiduciary responsibility with regards to cybersecurity (i.e. a duty of care)
- When states do adopt "cybersecurity laws" they are often frameworks for government action rather than provisions on what is required
  - US: Cybersecurity Information Sharing Act, FISMA, etc.
  - EU: Reg. (EU) 2019/881 – ENISA regulation

UNIVERSITÉ DU LUXEMBOURG

- Rules are different across jurisdictions
  - But some jurisdictions can have global effects, e.g. GDPR
- The problem
  - There is a duty as a reasonable prudent operator/actor/company/etc to secure information assets and IT systems
  - BUT there is little *legal* guidance as to what this means and a complete lack of regulatory certainty
    - This was a core challenge to the FTC use of its authorities to pursue data breaches

UNIVERSITÉ DU LUXEMBOURG

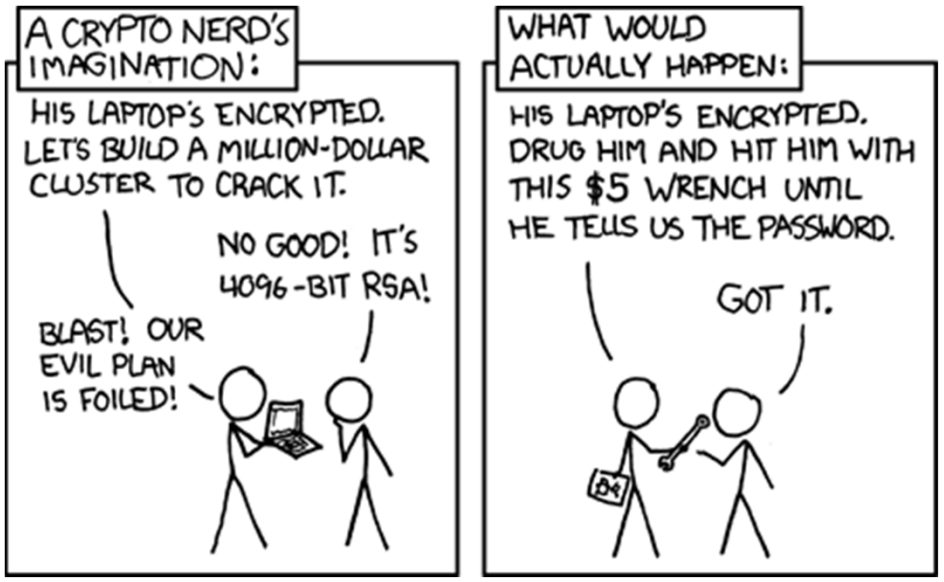
- To sum it up:

Thou Shalt be Cyber-secure.

UNIVERSITÉ DU LUXEMBOURG

UNIVERSITÉ DU LUXEMBOURG

- Some bad news
  - Your system is not secure and it will never be secure.
    - It can only be secure *enough*
  - Cybersecurity is an ongoing enterprise and must be constantly reevaluated
  - Threats and vulnerabilities are everywhere and multiplying



UNIVERSITÉ DU LUXEMBOURG

- Cybersecurity is about CYA
  - From a legal perspective this means that you need to be able to demonstrate that the company was fulfilling its duties with regards to cybersecurity
  - This is done through a variety of technical and legal mechanisms
    - Adherence to technical standards and certification
    - Internal policies
    - Contracts with vendors and customers
    - Technical implementations
    - Logging and penetration testing

UNIVERSITÉ DU LUXEMBOURG

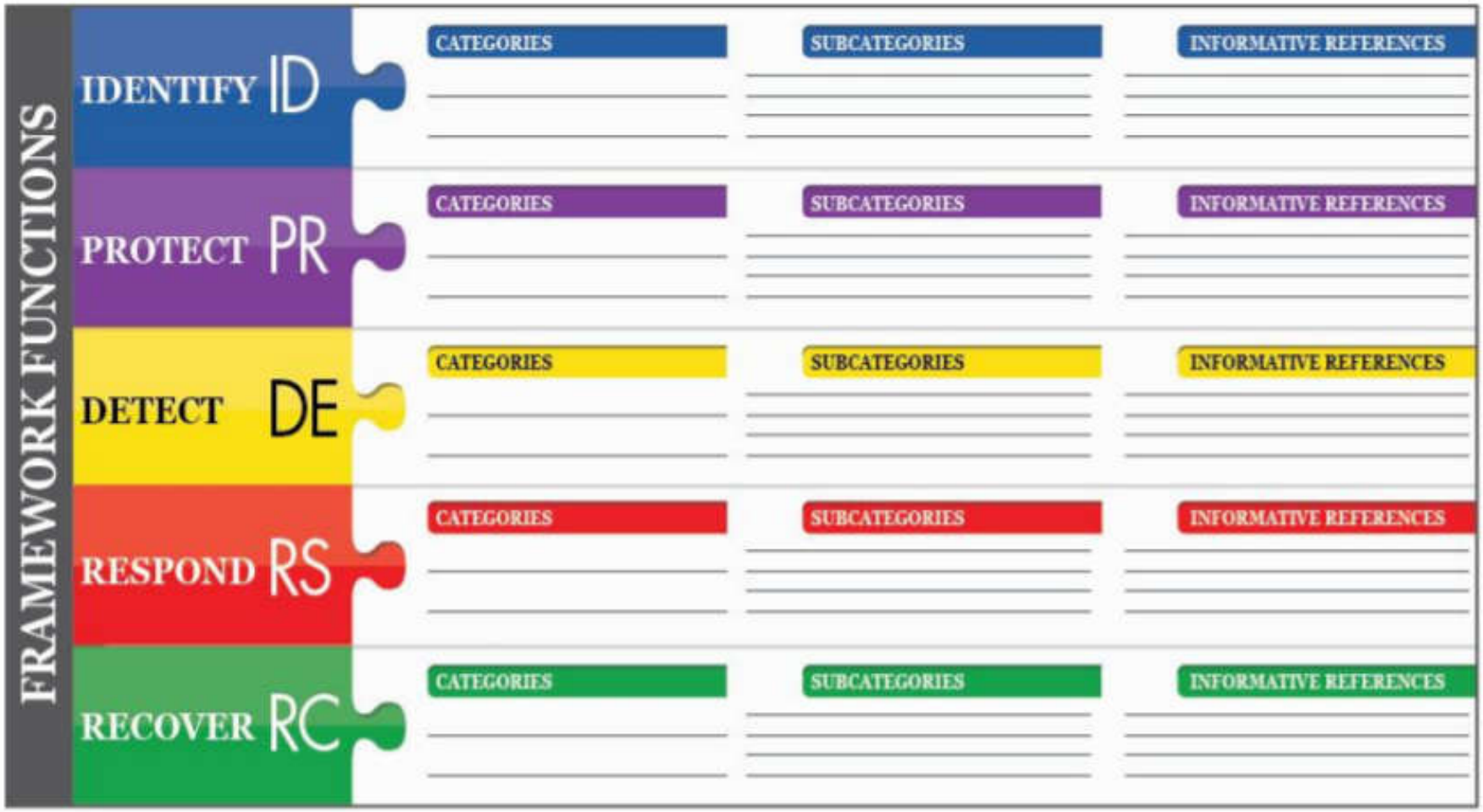
- Risk Assessment and Management
  - Cybersecurity requires you to identify and assess the risks
    - These can be legal, political, or technical
  - And mitigate these adequately based on the
    - Severity of the risk
    - Costs of addressing the risk
- For instance
  - Expending massive resources on securing the public facing website is likely a bad investment
  - Not encrypting the C&C uplink to a satellite because it is expensive is likely inadequate

- For example: ISO/IEC 27001 Certification
  - ISO/IEC 27001 is a technical standard that specifies how to implement an Information Security Management System
    - Certification in this standard is a powerful tool in showing potential contract partners that the company is securely managing its information assets alleviates some due diligence burdens
    - Standard details how to develop an ISMS plan and how to select controls that guide implementation
      - Policies that describe how the company is plans to manage information security AND
      - Technical implementation of these policies
    - This is a bespoke process: The standard itself helps to develop the plan through assessment of risk specific to the company; controls are then selected to implement the ISMS plan; and technical implementations are selected to achieve these goals
      - i.e. 1: we have PII on a server; 2. we will manage the risk by encrypting all PII in case of a data breach; 3. we will use RSA encryption to do this

- As a lawyer you can't do this alone! You need the ISM Team!
  - ISM Team – technical implementation and policies
  - Lawyers – reviewing internal policies and ensuring proper contract clauses

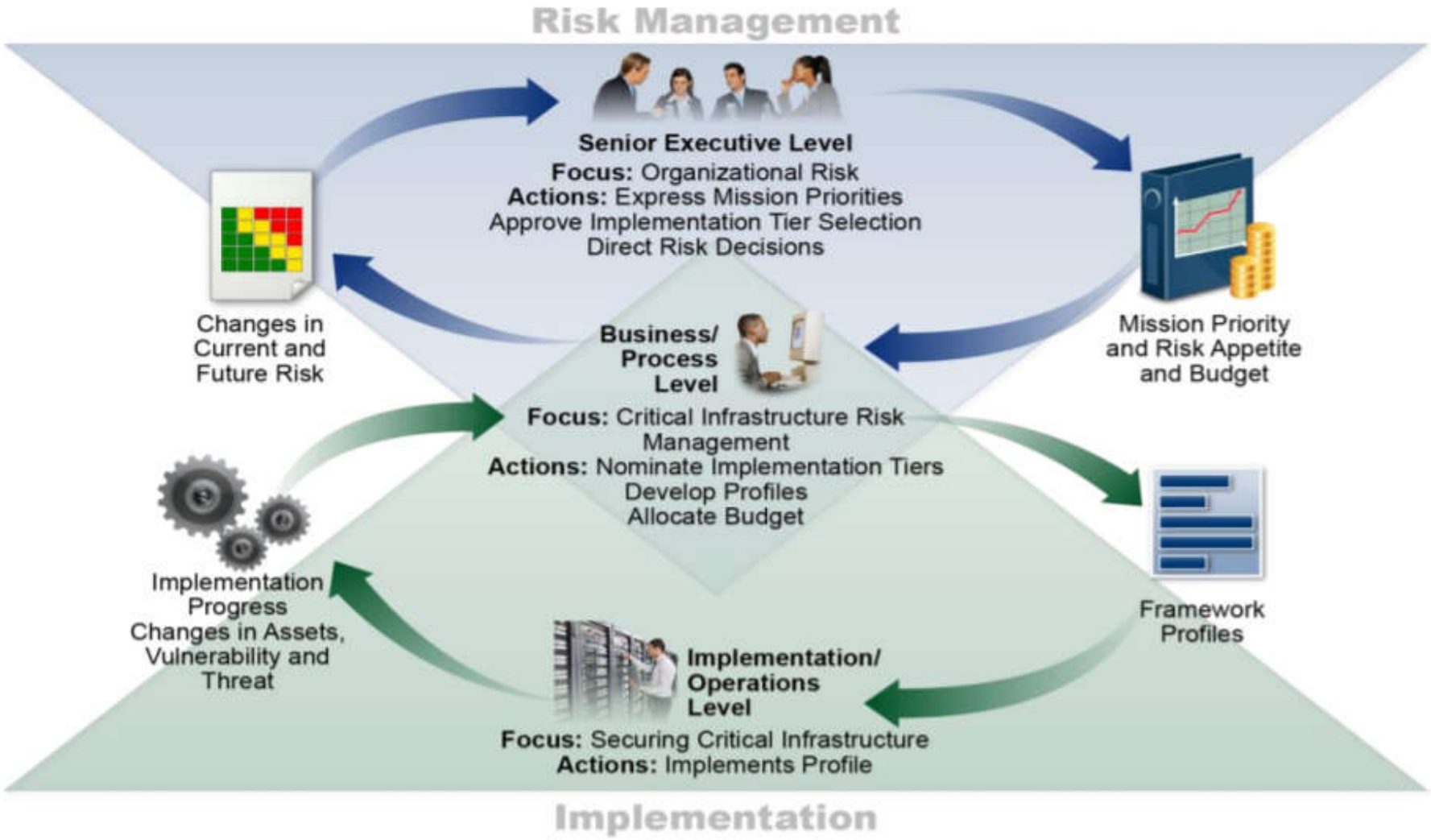
- Process – NIST Cybersecurity Framework

UNIVERSITÉ DU LUXEMBOURG



UNIVERSITÉ DU LUXEMBOURG

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8


Risk Management
Senior Executive Level
Focus: Organizational Risk
Actions: Express Mission Priorities
Approve Implementation Tier Selection
Direct Risk Decisions
Changes in Current and Future Risk
Mission Priority and Risk Appetite and Budget
Business/ Process Level
Focus: Critical Infrastructure Risk Management
Actions: Nominate Implementation Tiers
Develop Profiles
Allocate Budget
Implementation Progress Changes in Assets, Vulnerability and Threat
Framework Profiles
Implementation/ Operations Level
Focus: Securing Critical Infrastructure
Actions: Implements Profile
Implementation

Doing Cybersecurity

UNIVERSITÉ DU LUXEMBOURG

- Cybersecurity is Bespoke!
  - Industry requirements can effect what controls need to be implemented
    - Example: The financial Industry has specific data rules
  - The space industry is no different
    - Currently marked by a proliferation of satellites that are taking advantage of “cyber technologies”
    - Internet by satellite may allow users an uplink to a satellite in a way broadcast did not
    - Satellites are valuable targets for states and cyber allows attacks that avoid the debris problem
    - Supply chain threats: increase in use of COTS

UNIVERSITÉ DU LUXEMBOURG

- Cybersecurity in space industry
  - Industry level rules have lagged
  - This is due in part to the historical difficulty and remoteness of the space domain
- Industry specific action is emerging
  - Aerospace Industries Association - NAS9933: Critical Security Controls for Effective Capability in Cyber Defense
  - Committee on National Security Systems – Security Standards for US DoD
  - Consultative Committee on Space Data Systems – Standards on Space Data
  - Space ISAC – US initiative
- But the space industry still lags in this area

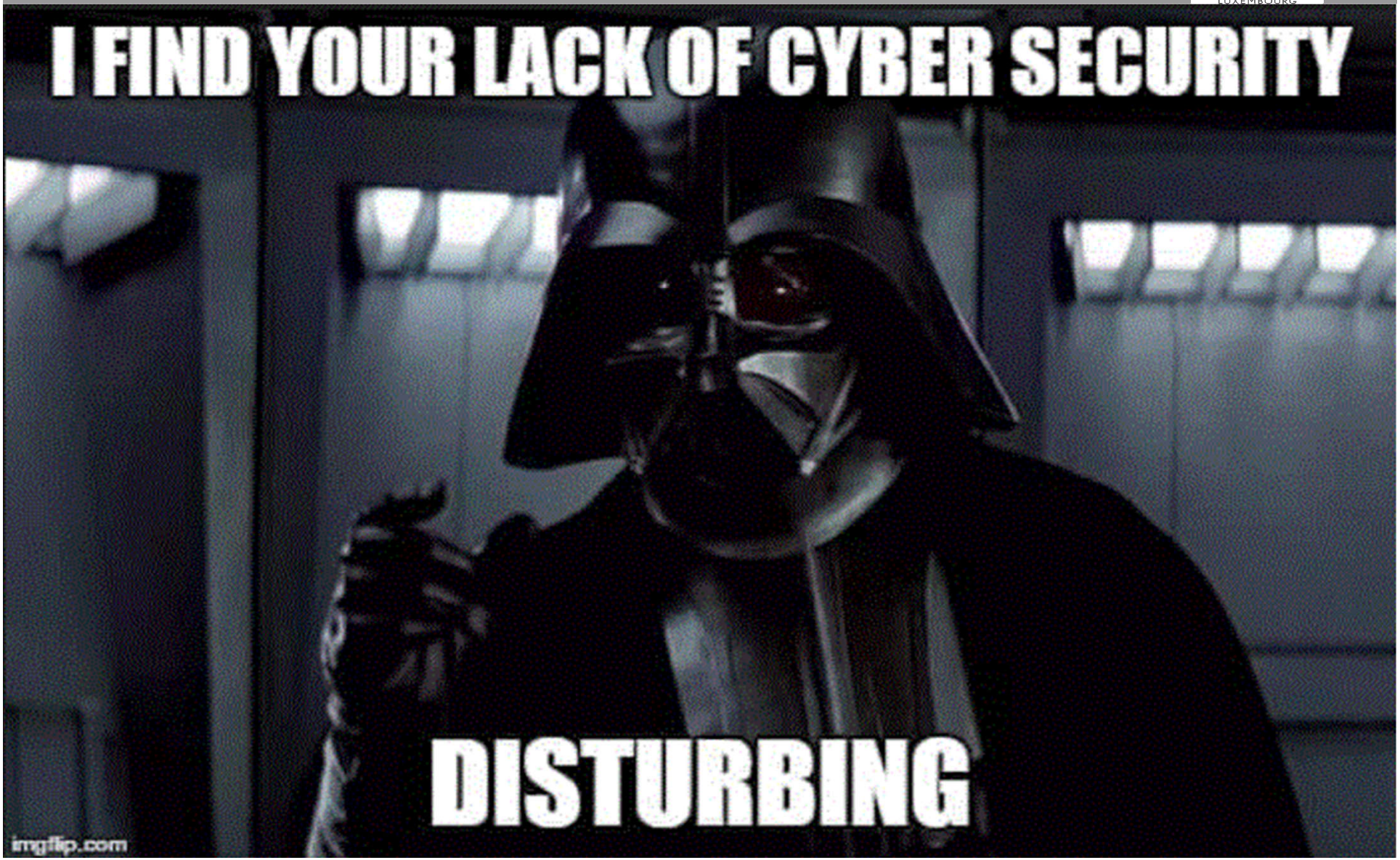
Data Risk	System Risk	Legal/Political Risk
National Security Information	Propulsion	ITAR
Proprietary Information	Imaging Capabilities	GDPR
Protected information	Communication Links	Shutter Control
	SigInt	Responsibility/Liability
	Ground Station Vulnerabilities	National Security

Currently there is no baseline guidance specific to space systems on assessing risk.

University CubeSat ≠ GovSat

- The good news: Cybersecurity is flexible and adaptable – using frameworks such as the NIST Cybersecurity Framework or ISO 27001 can guide operators in risk assessment and management
- BUT: there needs to be increased information sharing and discussion on specific standards/tools for cybersecure space operations
  - Insecurity for any one operator can mean insecurity for other operators – it is a space debris-esque issue
- There also needs to be international cooperation on reestablishing rules of non-interference in space
  - Unlikely
- Finally, as innovation of new applications in space continues, the needs for cybersecurity will increase
  - i.e. just imagine the chaos a hacked Starlink system could cause

Cybersecurity for the Space Industry



Stay connected with us!

pjblount@gmail.com

percy.blount@uni.lu

@blountsfolly