Cybersecurity from operations point of view

G. GALET – DNO/OP

AGENDA

- Context of CNES Space Operations
- Space System overview
- Ground Segment development
- Ground Segment management / maintenance
- Mission management point of view
- Conclusion

ANECDOTE

Confidentiality ?

Limit between allowed / forbidden ?

Better not to speak !

We are not informed of everything …

This is not our role !

We just do what we are told to do !

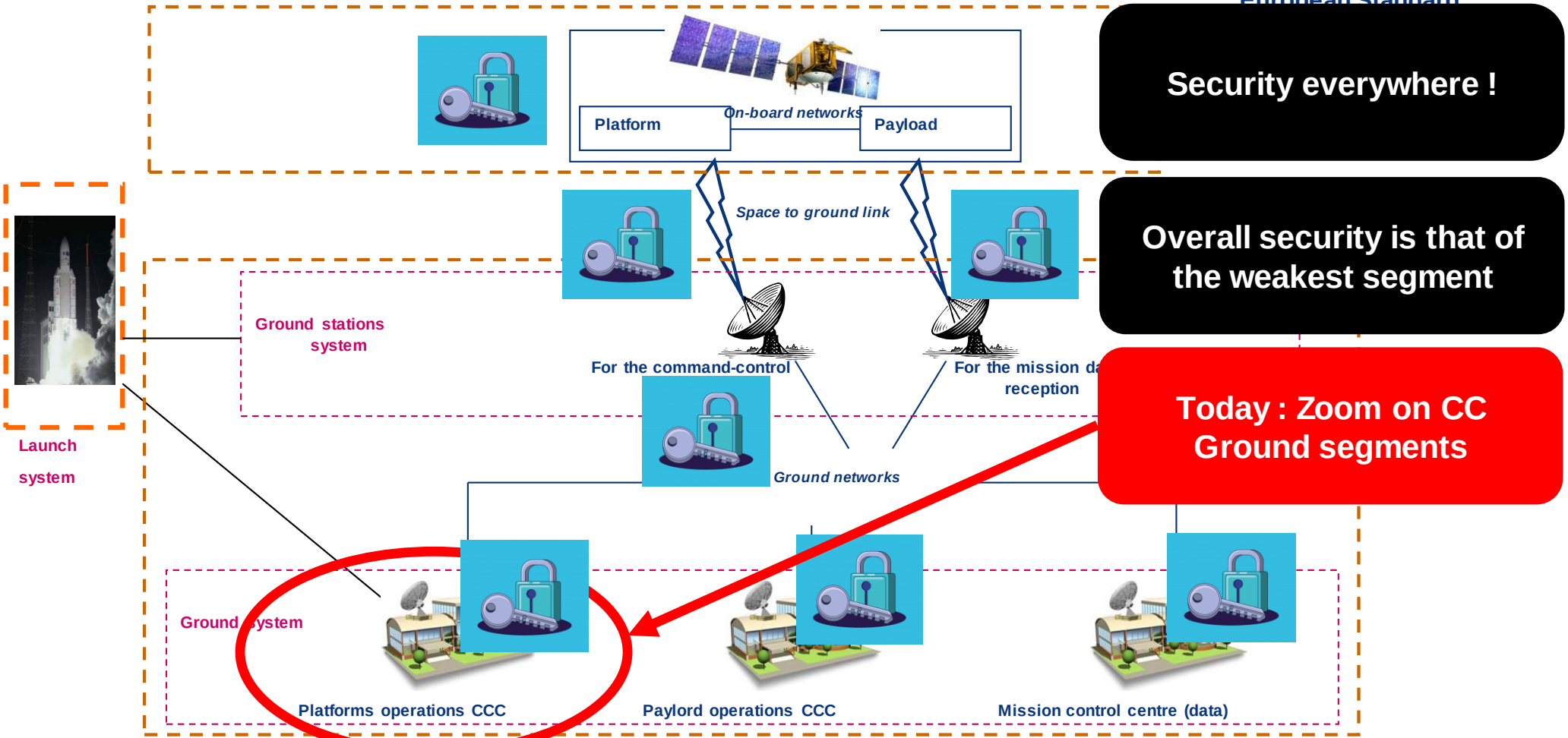
Thus not so simple to adress this point of view (on behalf of the ops teams)

CONTEXT OF CNES SPACE OPERATIONS

Many different requirements for various missions typologies

- **Military** missions : High Level constraints => Ops network fully segregated / "Bunker" …
- **Dual** missions : Nearly as for military missions
- **Civil** missions for science / altimetry, etc. : Mainly secured for mission availability requirements
- **Instruments** operations (on Mars, Comet etc.) : Mainly remote Ops via VPN – Security imposed by the main Ground Segment owner

SPACE SYSTEM OVERVIEW



Security everywhere !

Overall security is that of the weakest segment

Today : Zoom on CC Ground segments

GROUND SEGMENT DEVELOPMENTS (1/2)

- **Security must be considered from the very beginning of the project**
  - Based on the sensibility level of data, the future interconnections of the GS, the securisation of the ground to space link, etc.
  - Definition of adequate solutions in the GS architecture and components (networks segregation, DMZ, limited fluxes, etc.)
  - Challenge is to anticipate the best as possible without sur-evaluating the required security level
- **Security impacts on all the GS components / layers must be evaluated**
  - From virtualization, operating systems, SW parts, etc
  - Choice of adequate solutions in terms of authentication, anti-virus, configuration management, logbooks to be developed
  - Challenge is to optimize the trade-of between security & future GS exploitability and to consider the induced costs in the project

GROUND SEGMENT DEVELOPMENTS (2/2)

- **Interface with the S/Co is very important :**
  - Collaborative work to converge on the security requirements
  - Appropriation / Implementation by the S/Co in terms of means (HW / SW / Networks, teams, trainings.)
  - Common definition of the data exchanges protocols
  - To share the good practices on both sides *(such as different anti-virus on both sides)*
- **Future security homologations must be considered and prepared very well in advance**

Key of success : Close collaborations between GS developers and CYB experts at all levels (customer, prime, S/Co, etc.)

GROUND SEGMENT MANAGEMENT / MAINTENANCE (1/4)

- Security Requirements are defined by the project with CYB architects
- Operational actors must respect these requirements
- Verification is permanent : From acceptance tests up to regular security audits
- Dedicated CYB support all along the project live
- In case of non compliance, possibility to manage temporary waivers
- Full configuration management and full traceability for proper security management
- 1st level = Security part of CCC supervision => associated real time monitoring defined from the beginning => Alarms – Mainly for equipment's connection / disconnection, logins / pwd, identification of data fluxes, etc. => Manageable by Ops team and then reporting to CYB support => Mainly Human loop
- 2nd level = Dedicated security logs (mainly for inquiry) – Relationship between Ops teams and CYB support very vital as security logs not necessarily accessible and/or understandable for Ops actors – Not necessarily analyzed in Real Time

GROUND SEGMENT MANAGEMENT / MAINTENANCE (2/4)

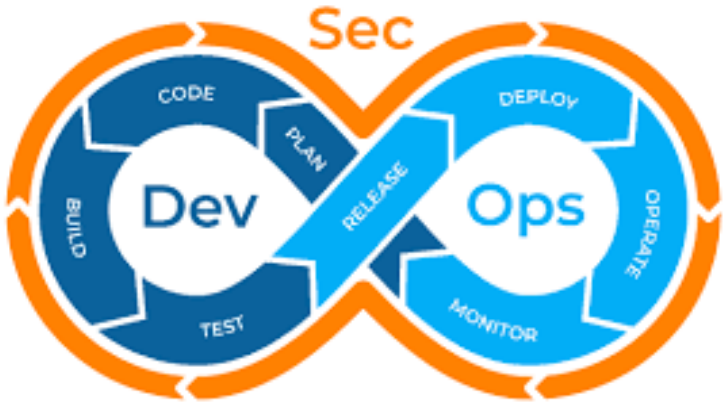
- **Security requirements can be constraining for operations optimization, such as :**
  - Generic logins for better operators hand-over without ops processes interruption versus personal logins
  - Password changes (up to every 3 months) : Strict management to be sure to be able to connect (in particular for on-call actors during nights)
  - Management of evolutions : Mainly integration of Costs, SW updates – Necessity to segregate Development area from Ops area !! Very constraining for reactivity
  - Permanent compromise between security updates and regression risks on operational SW
  - Systematic control of external supports before connection to the ops network (but urgency …)
- **In some way, defense mission are optimized for security but not for operations (remote off-line analysis, assessment from outside, valorization of these operations, etc.)**
- **Up to now, no mission impacts assigned to CYB problems on our in-flight missions**

GROUND SEGMENT MANAGEMENT / MAINTENANCE (3/4)

- **The keys of success :**
  - Pertinent conception of security from the beginning : At the proper level with consideration of the operational constraints (CCC components, organization, Ops concepts, etc.)
  - Good partnership between Ops actors and CYB supports
  - Trainings / explanations for Ops actors : Not to consider CYB as a constraint
  - Full transparency even with events appears as not critical

GROUND SEGMENT MANAGEMENT / MAINTENANCE (4/4)

- **Axis of improvement**
  - To better explain the CYB requirements to Ops actors
  - To better involve the Ops actors in the CYB management (access to logs, explanation)
  - To perform security logs monitoring in Real Time : Via new generation of SOC ? What about transfer of logs ?
  - To easy the management of evolutions : towards DEVOPS ? Or more DEV**SEC**OPS ?



MISSION MANAGEMENT POINT OF VIEW (1/2)

- Management of information not easy due to networks segregation
- Reduction of data traffic between Ops area and outside : limitation to the strict minimum required
- Communication means very restricted : strong constraint in particular for young operators (connected generation)
- Management of Anti-virus by operators because ops area not connected to the company IT network (for defense mainly)
- Passwords management : Not so simple (old habits to be prohibited such as the post-it !!)
- Security devices not necessarily up to date and they must last decades !!!

MISSION MANAGEMENT POINT OF VIEW (2/2)

- **Axis of improvement (mainly for defense missions)**
  - To adapt the security of Ops Support networks to the proper level in order to ease the data exchanges with the Ops support

  - To implement modern devices for ops actors identification (w/o passwords) such as biometrics systems etc.
  - To improve the SW costs monitoring for better anticipation of potential problems

SYNTHESIS

- The current situation is acceptable for our in-flight missions as we can not assign impacts due to CYB problems
- The internal organization is vital for good collaboration between Ops and Cyb actors => To encourage team building initiatives (social events, co-localization…)
- The are some axis of improvements in particular to move towards DevOps logic => Proposal to set up a dedicated COMET day on DEVSECOPS
- Security is required to evolve rapidly => Ops actors must be in the loop to find optimized solutions / organizations

LAST BUT NOT LEAST

From the Ops point of view, the topic of the day is not easy to address in an open COMET day !!!!

THANKS …