

Towards Developing Resilience and Cyber-Physical Protection Capabilities in Aviation Critical Infrastructures

March 2021
Athens, Greece



Georgia Lykou

Athens University of Economics & Business, Greece

Research Area & Contributions (1)

Research Question:

*Interdependency Analysis,
Tools and Methodologies
developed for CIP?*

Research Question :

*- Is Transport Sector Resilient to
Climate Change Impacts?
- How to increase sustainability?*

Transport Sector CIP

Time-based critical infrastructure
dependency analysis for large-scale
and cross-sectoral failure

Classification and
Comparison of CIP
tools

Cybersecurity Self-Assessment
Tools for Industrial Control
Systems

Climate Change Impact
Analysis in Transport

Analysis and Classification
of Adaptation Tools

New Methodology for Data
Centers Sustainability
Assessment

- 3 Internat. Journal Publications
- 6 International Conference Papers



Research Area & Contributions (2)



Research Question:

**Is Aviation Sector
Cyber-Resilient?**

**Aviation Sector Resilience &
Cyber-Physical Protection**

**Airport's Cyber-
Security
& Cyber-Resilience**

**Air Traffic
Management
Cyber-
Resilience**

**UAS & IoTs
Cyber Risks
in Aviation**

**Assessing
Interdependencies and
Congestion Delay Risk
in **Aviation Network****

- 3 Internat. Journal Publications
- 1 International Conference Paper
- 1 Book Chapter Publication



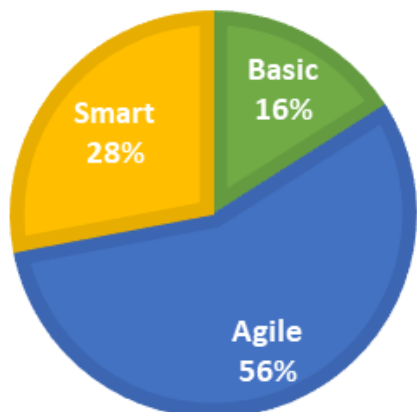
Smart Airports Cybersecurity: Measures to Improve Cyber-Resilience

Research Methodology

- Combination of literature research and **Online Survey**
- Research goal: implementation rate of Cyber-Security Best Practices for IoTs
- Great diversity of technological evolution in airports

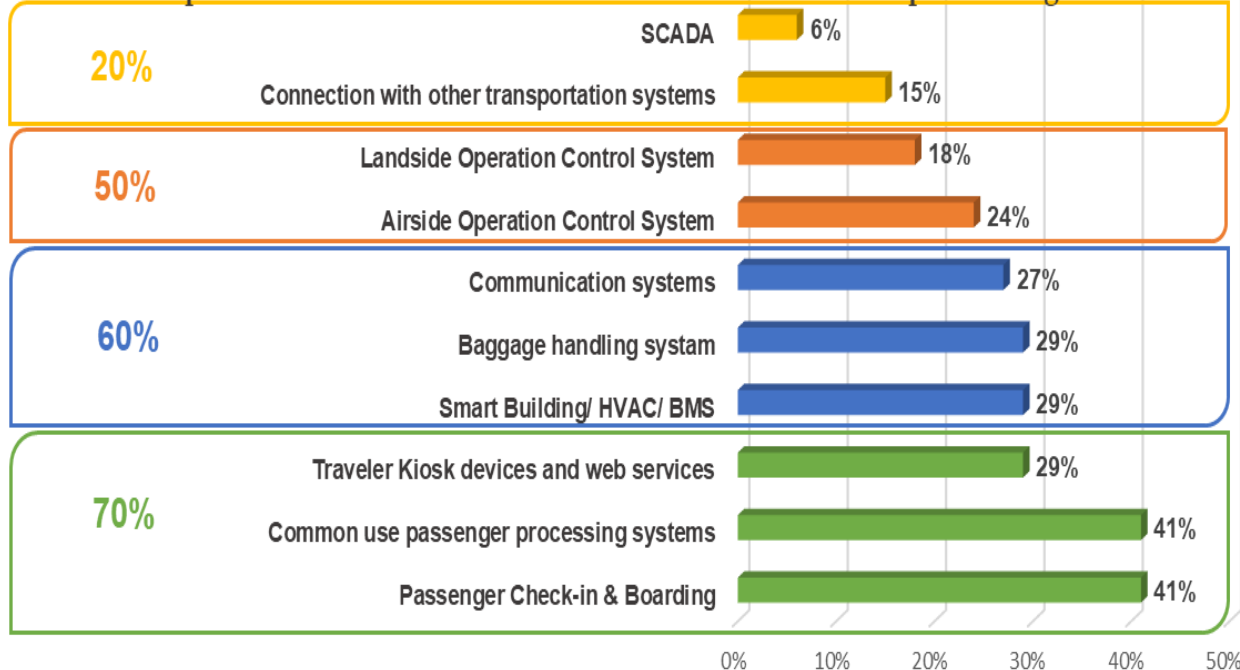
AIRPORTS CLASSIFICATION

■ Basic ■ Agile ■ Smart



In Smart Airports

In All Airport's Categories



Conference Paper:

Lykou G., Anagnostopoulou A., Gritzalis D., *“Implementing cyber-security measures in airports to improve cyber-resilience”*, in Proc. of the Workshop on Industrial Internet of Things Security (WIIoTS-2018), Spain, June 2018

Smart Airports Cybersecurity: Developing Cyber Resilience

Seven (7) Attack Scenarios with Mitigation and Resilience Measures

Malicious Attack Scenarios:

1. Distributed Denial of Service attack
2. Communication Attack to ATM Systems
3. Malicious Software on an Airport's Network
4. Tampering with Airport Self-Serving Systems
5. Network attack to CCTV systems
6. Misuse of Authorization
7. Email Phishing and Social Engineering Attacks

Step 5: Server ignores legitimate requests



Step 3: Botnet makes requests to airport's server for a specific service



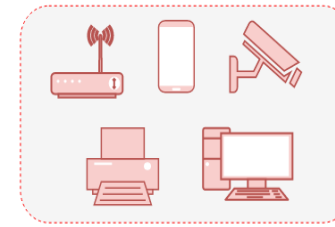
Step 6: Exhaustion of server's resources leads to unavailability of the server



Step 4: Legitimate user makes request to airport's server



Devices are enlaved into an arrangement (known as Botnet)



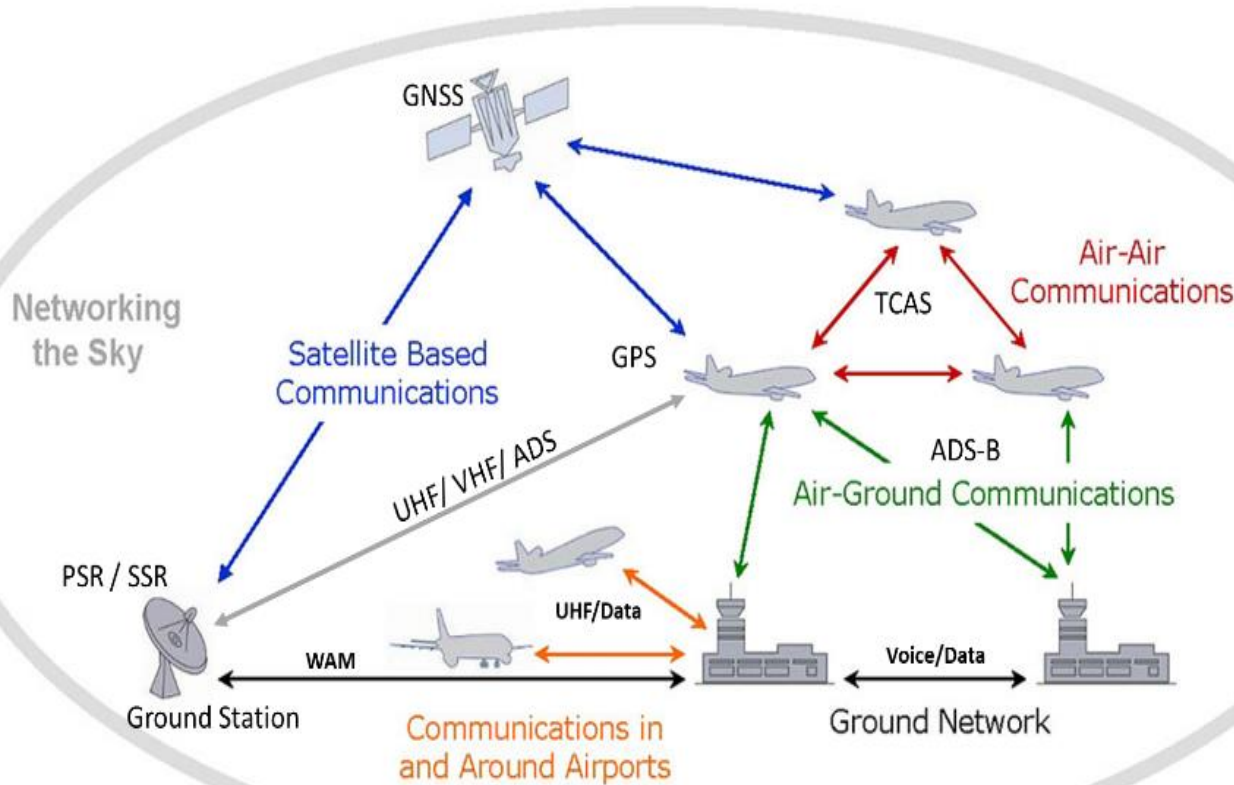
- Impact Evaluation
- Cascading effects
- Mitigation Actions
- Resilience Measures

Journal Paper:

Lykou G., Anagnostopoulou A., Gritzalis D., "**Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience**", SENSORS, January 2019

Aviation cybersecurity & cyber-resilience in Air Traffic Management (ATM) Systems

ATM systems serving communication, navigation, surveillance and ATM interoperability for air traffic control:



- Air –Ground Voice Communications & Data Links
- Primary and Secondary Surveillance Radars (PSR/SSR)
- Automatic Dependent Surveillance-Broadcast (ADS-B)
- Traffic Collision and Avoidance System (TCAS)
- Wide Area Multilateration (WAM)

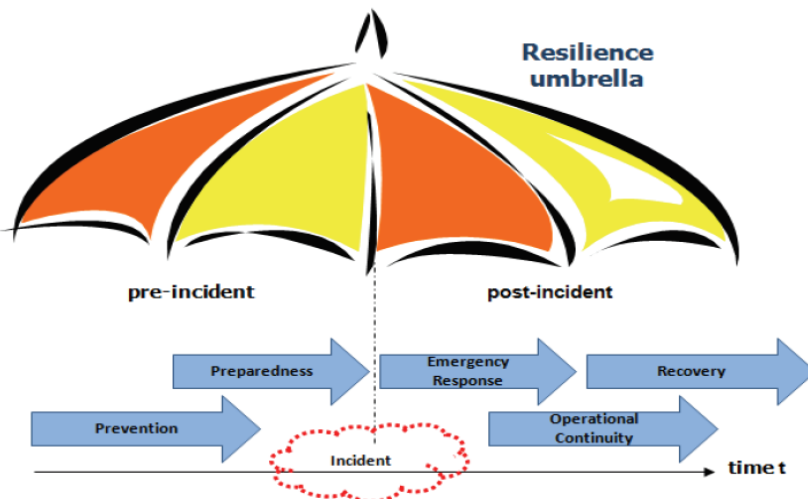
Book Chapter:

Lykou G., Iakovakis G., Gritzalis D., "**Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management**", in Critical Infrastructure Security and Resilience, Gritzalis D. et al. (Eds.), pp. 245-260, Springer Book: Advanced Sciences and Technologies for Security Applications, 2019.

Aviation cybersecurity & cyber-resilience in Air Traffic (ATM) Systems

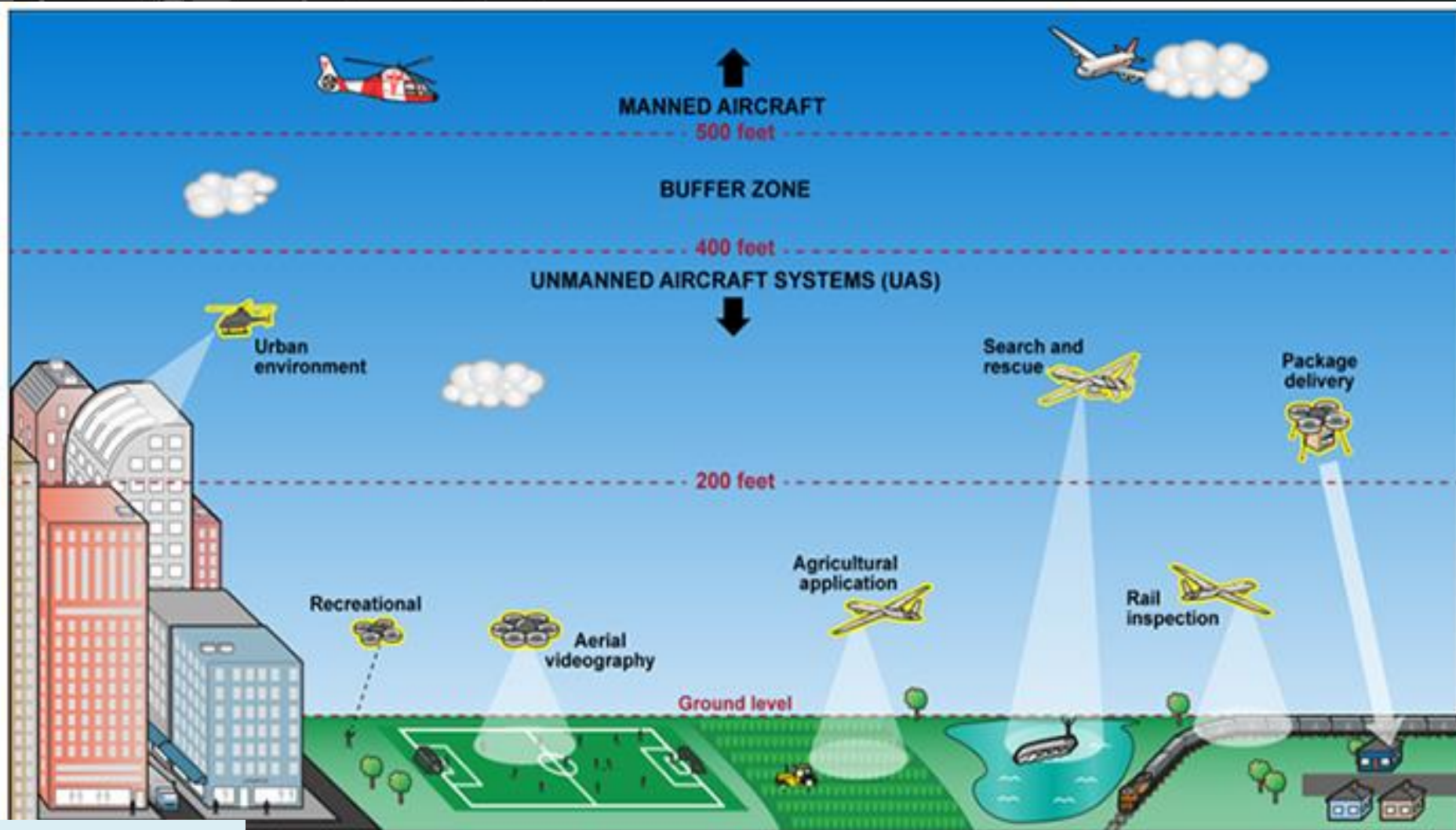
Research Contribution :

- An extended threat model for analyzing aviation targets and risks involved.
- Introduce and analyze cyber resilience aspects in the aviation with holistic strategy for defense, prevention and response.
- Introduce Resilience Measures for all ATM actors to work on collaborative, address security threats, and increase the aviation systems resilience



Threat	Resources	Goal Motivation	Capabilities	Hardware Cost	ATM Target	Risk
Passive Observers	Very low	Information collection Financial or personal interest	Eavesdropping, use of website & mobile apps.	Internet access, SDR receiver stick (\$10)	ADS-B	Low
Hactivists & Hobbyists	Low	Any noticeable impact Thrill and recognition	Eavesdropping, replay attacks, denial of service.	COTS SDR transmitter (\$300-\$2.000)	ADS-B	Low
Insiders	Low - Medium	Disgruntlement, Revenge, Maximise financial gains selling proprietary information	Resources for specific impact on operations, based on proprietary knowledge	Low cost, enforced by inside use of tools and info on security gaps	SSR, PSR, ADS-B, TCAS	Medium
Cyber Crime	Medium - High	Maximising impact Financial gains using e.g. blackmail or valuable information	Resources for large-scale operations with sophisticated transponders.	Directional antennas, small UAVs with SDR transmitters (~ \$5.000)	SSR, PSR, ADS-B, TCAS	Medium
Cyber Terrorism	Low - Medium	Political or religious motivation Massive disruption and casualties	Resources for specific high-impact ops, though usually on a limited scale	As with cyber crime, potentially on a smaller, more targeted scale	SSR, PSR, ADS-B, TCAS	High
Nation State	Unlimited	Weapons Targeting specific, potentially military objects	Anything physically and computationally possible	Military-grade radio equipment, capability for electronic warfare	SSR, PSR, ADS-B, TCAS, WAM	High

Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies

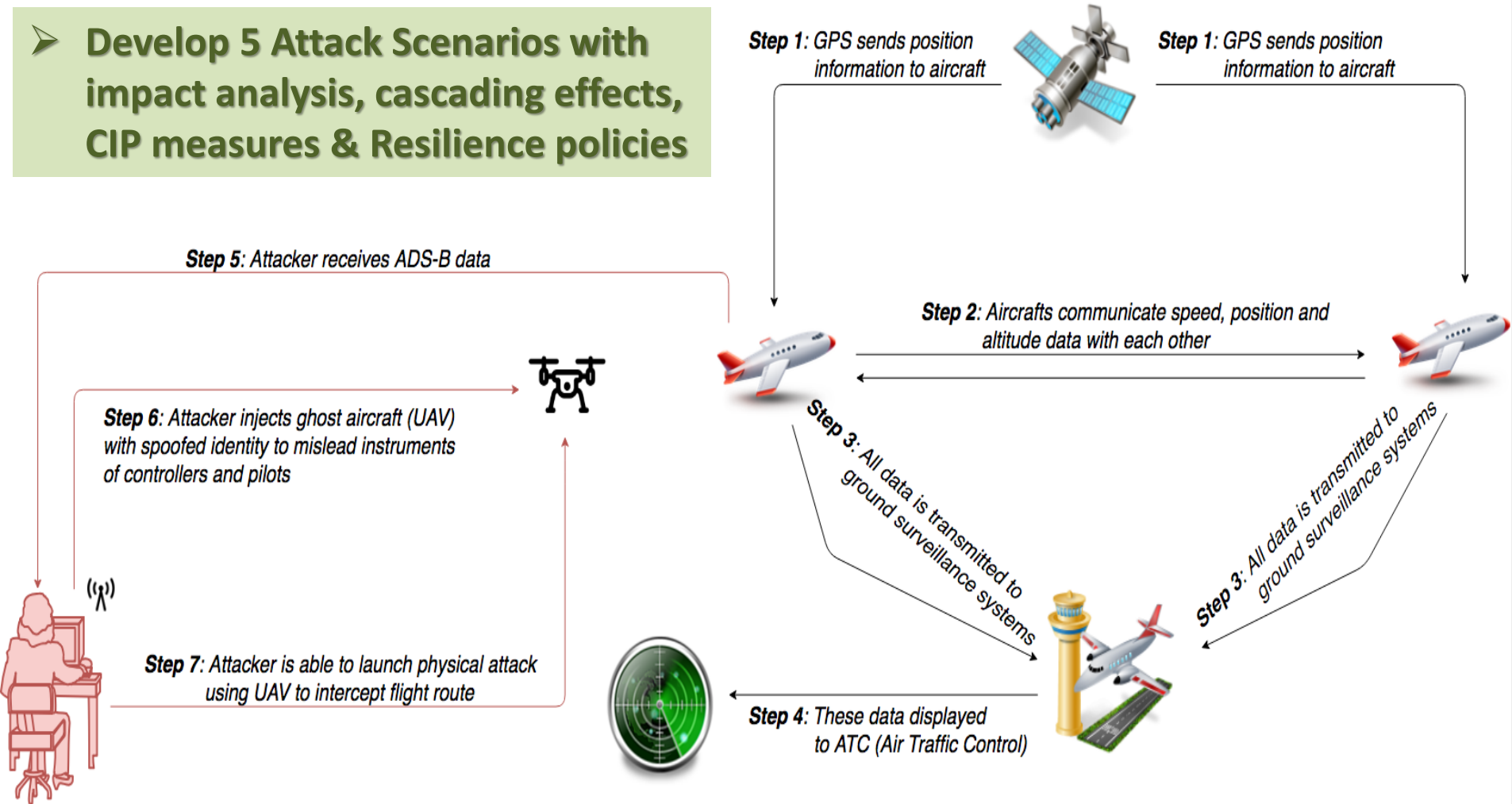


Journal Paper:

Lykou, G., Moustakas, D., Gritzalis, D., "*Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies*", Sensors, Vol. 20, No. 12, 2020.

Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies






➤ **Develop 5 Attack Scenarios with impact analysis, cascading effects, CIP measures & Resilience policies**






**Communication attack on ATM systems
Attack Scenario to Airport facilities**

Survey on Counter Drone (C-UAS) Sensors & Technologies







Sensors:

-  Acoustic
-  Visual/EO
-  Thermal
-  Radio Frequency (HF, VHF, UHF)
-  Radar

Kinetic Solutions:

-  Laser
-  Projectiles
-  Net

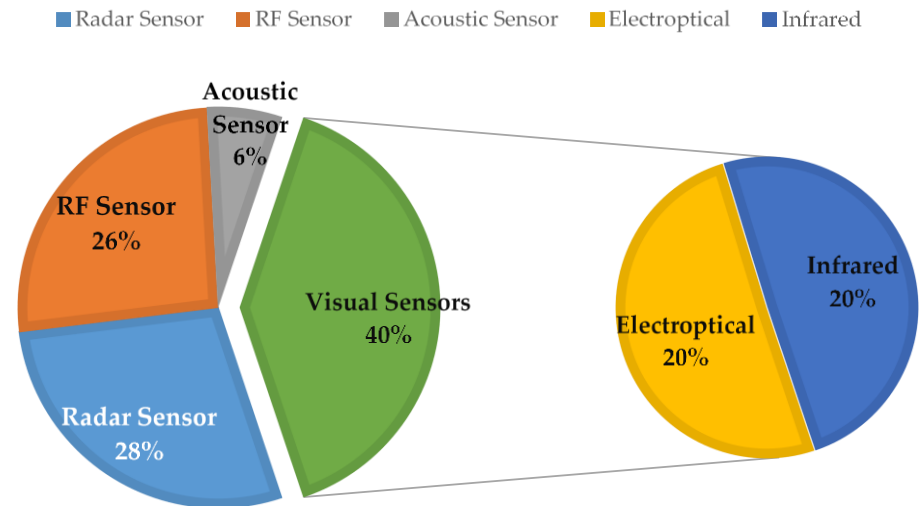
Non-interactive¹ Response:

-  Drone Alarms
-  Close Window Blinds
-  Shut Down Wi-Fi
-  Evacuate an Area
-  Deploy a Fog Grenade
-  Blind the Drone Camera

Non-Kinetic Solutions:

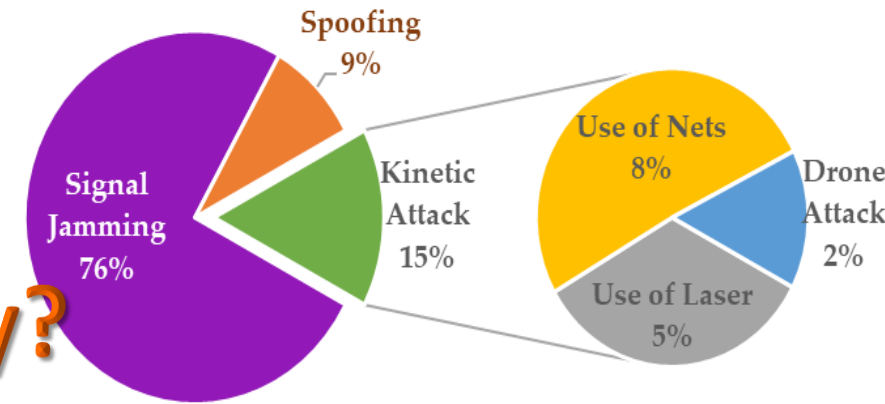
-  RF/GNSS Jamming
-  RF/GNSS Spoofing

SENSOR TYPE IN DETECTION SYSTEMS



545 C-UAS

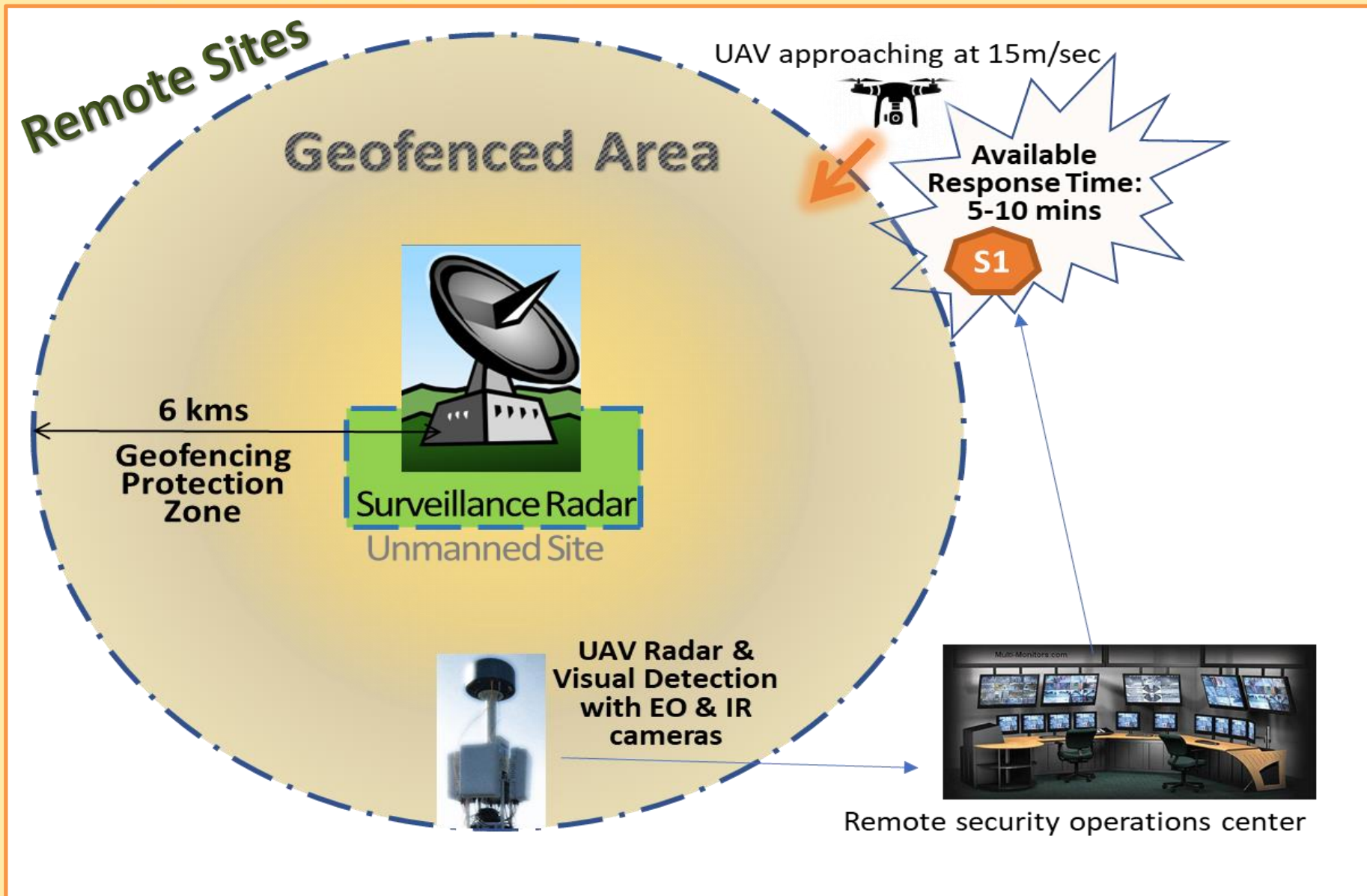
C-UAS Technology used for Mitigation



Airport Applicability?



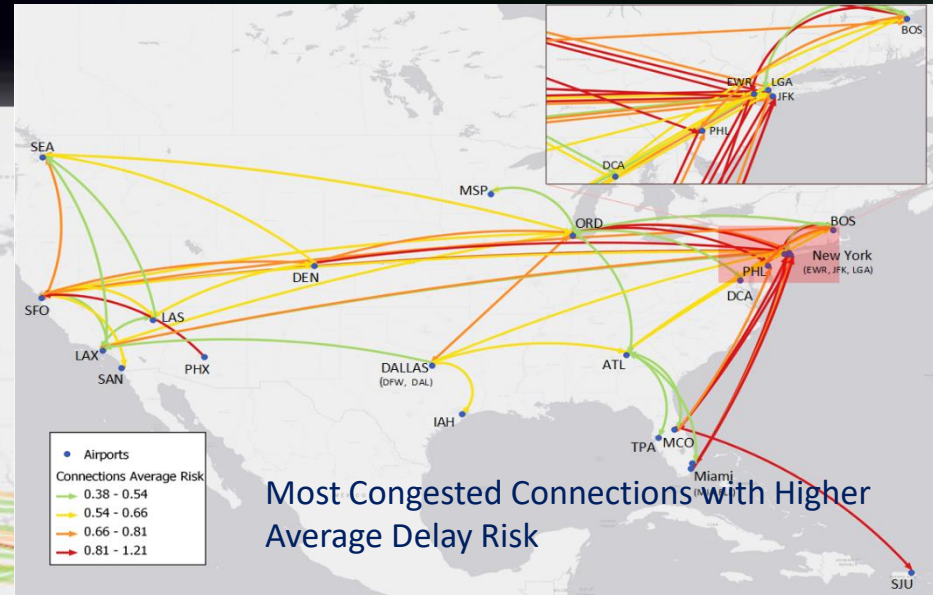
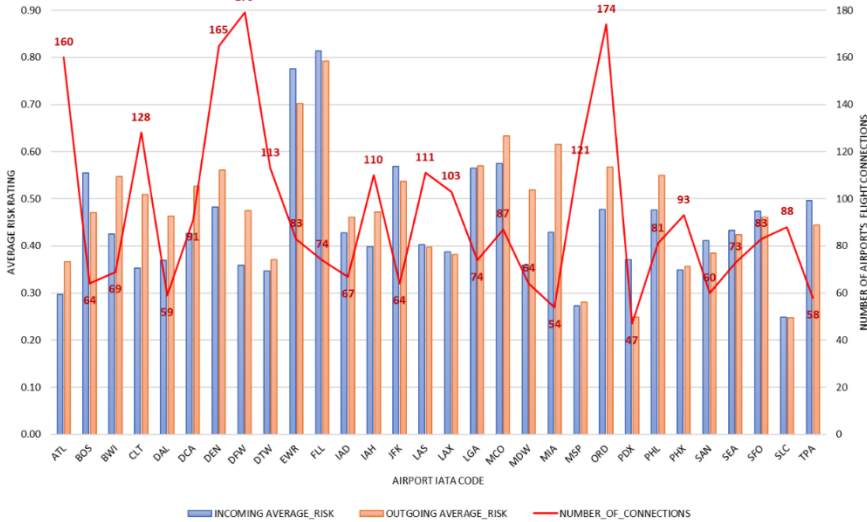
Proposed counter measures for airports & ATM Facilities



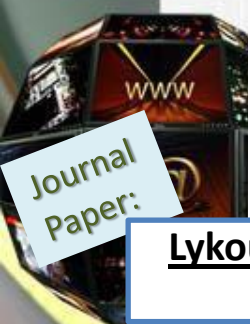
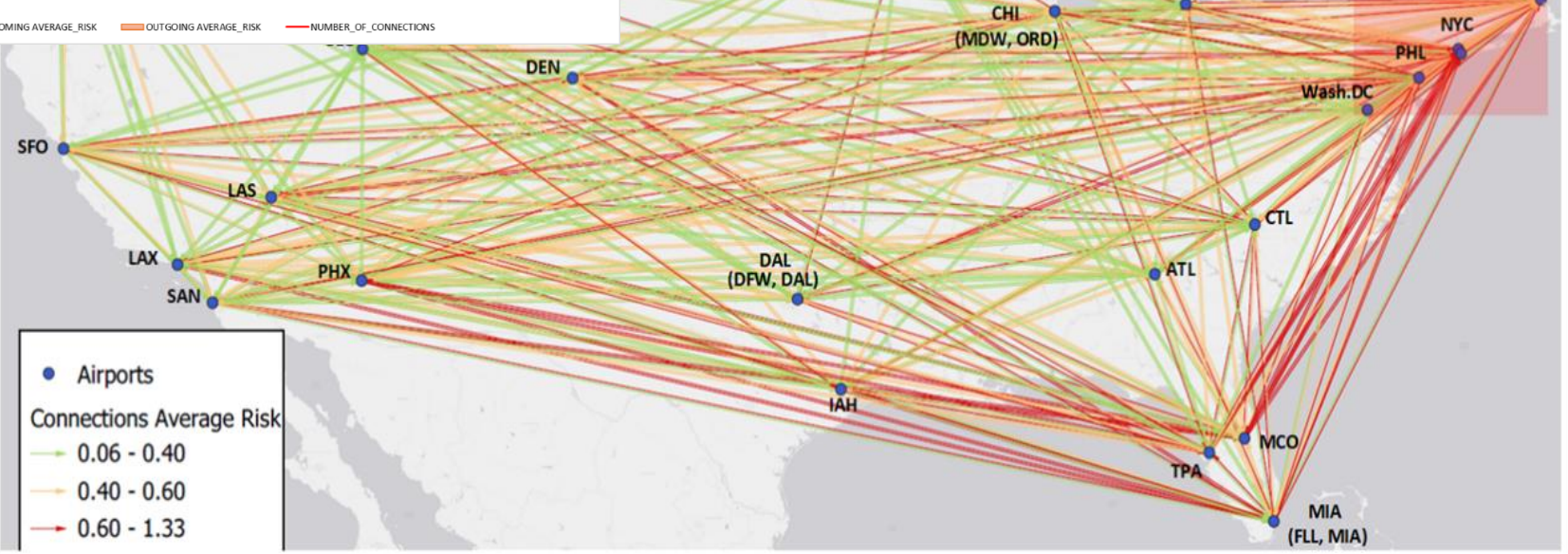
Assessing Interdependencies and Congestion Delays in the Aviation Network

July & August 2019

30 Busiest US Airports with Incoming and Outgoing Average Congestion Risk

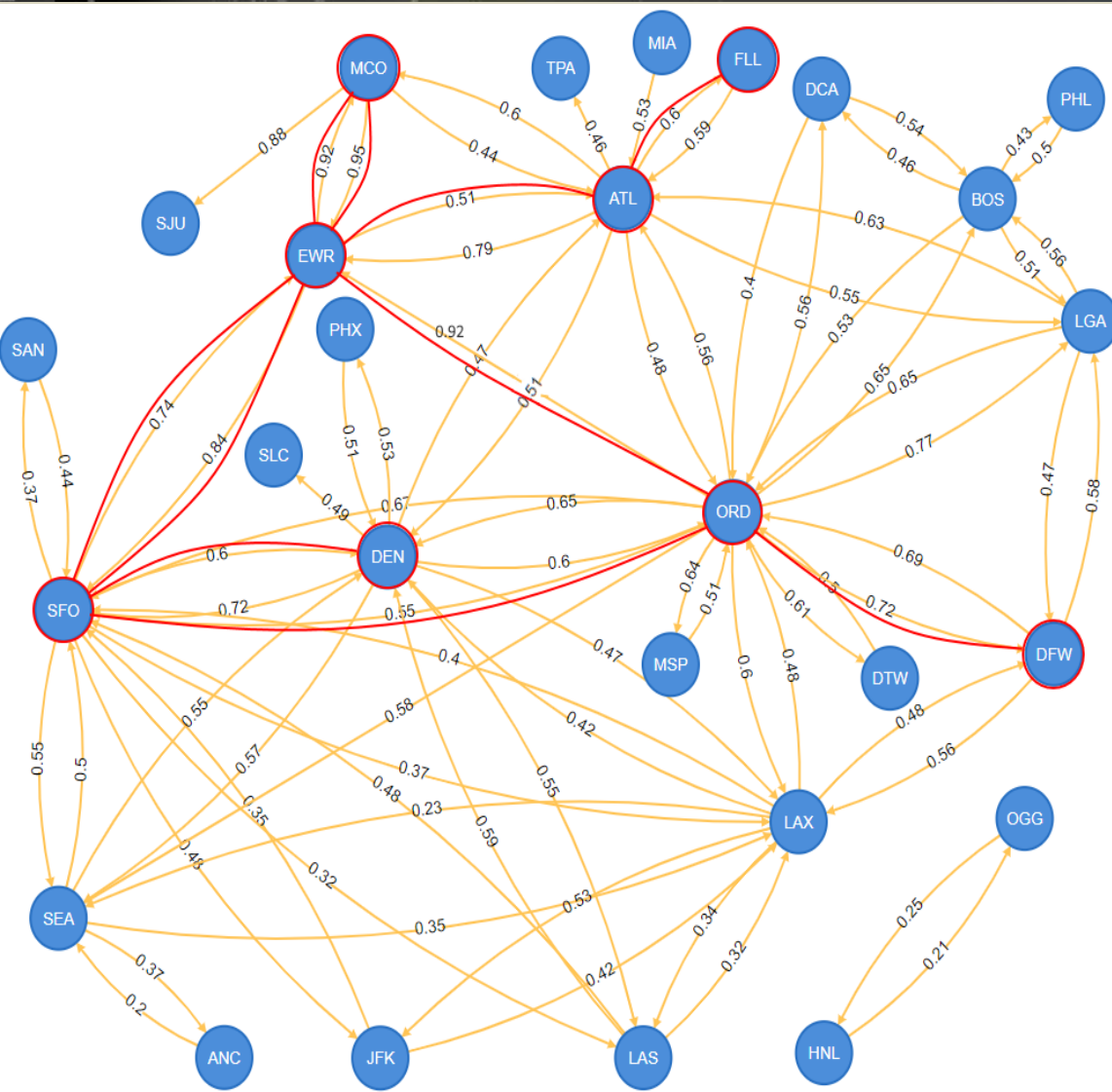


Most Congested Connections with Higher Average Delay Risk



Lykou G., Dedousis P., Stergiopoulos G., Gritzalis D., "Assessing Interdependencies and Congestion Delays in the Aviation Network", IEEE Access, December 2020

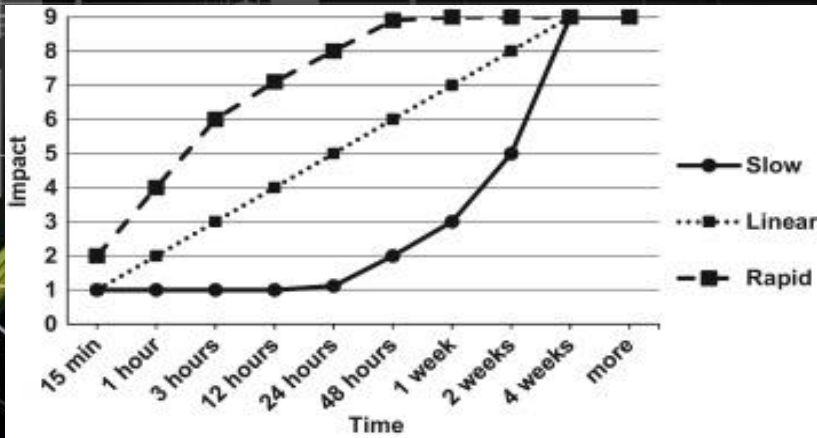
Assessing Interdependencies and Congestion Delays in the Aviation Network



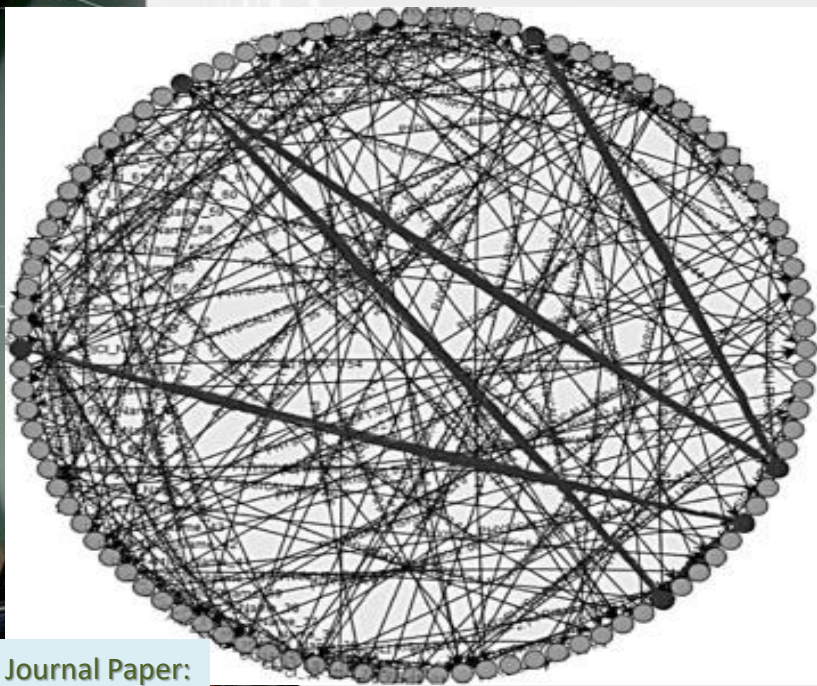
- ✓ Indicate the flight connections with highest delay risk
- ✓ Identify the worst n-order airport dependencies
- ✓ Analyze what-if scenarios for the congested airport's connections.
- ✓ Propose the n-order dependency chains, to be avoided by flight planners
- ✓ Reduce delay impacts in aviation networks.

Paths	Cumulative Risk
(ORD)→(EWR)→(MCO)→(EWR)→(SFO)→(DEN)	1.63
(ORD)→(EWR)→(MCO)→(EWR)→(SFO)→(EWR)	1.63
(EWR)→(MCO)→(EWR)→(SFO)→(EWR)→(ATL)	1.59
(EWR)→(MCO)→(EWR)→(SFO)→(ORD)→(DFW)	1.58
(MCO)→(EWR)→(SFO)→(EWR)→(ATL)→(FLL)	1.53

Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures



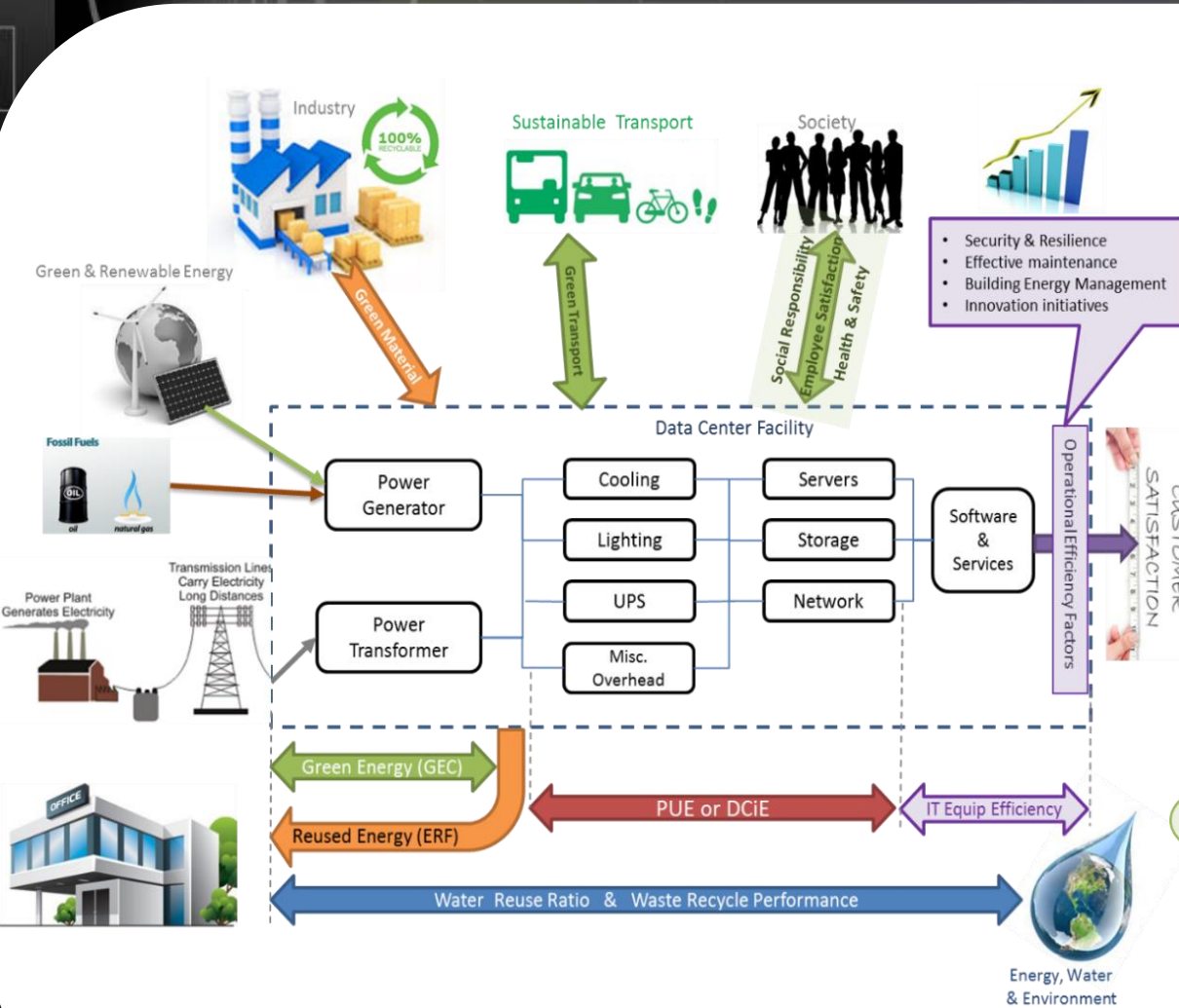
- Risk analysis methodology for cascading failures
- Different growth models (slow, linear and fast evolving effects)
- Failures triggered by concurrent common-cause cascading events
- CIDA: Critical Infrastructure Dependency Analysis Tool
- CIDA evaluates alternative defence strategies for complex, large-scale & multi-sectoral dependency scenarios



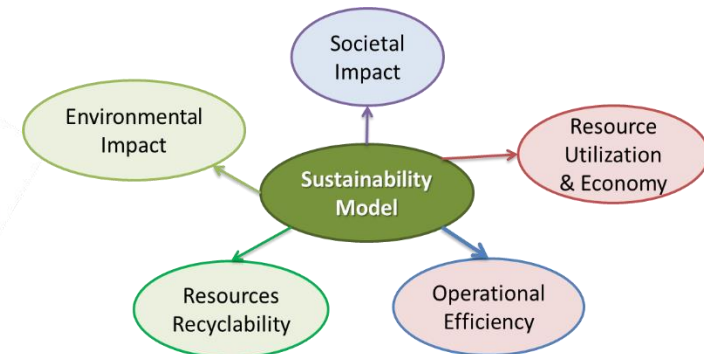
Journal Paper:

Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "*Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures*", Intern. Journal of Critical Infrastruct. Protection, March 2016

New methodology toward effectively assessing data center's sustainability



a/a	Sustainability Element	Influencing Factor (Fi)	Range	MAX Rating (Wi)	%	
1	Environmental Impact	GEC	0 ~ 1	15	75	
2		GMU	0 ~ 1	10		
3	Resource Utilization & Economy	DCiE	0 ~ 1	15		
4		ERF	0 ~ 1	10		
5	Resources Recyclability	Waste Recycle Rate	0 ~ 1	5		
6		Water Reuse Rate	0 ~ 1	5		
7	Operational Efficiency	IT Equipment Efficiency	0 ~ 1	15	25	
8		Security & Resilience Plan	Y/N	4		
9		BEMS	Y/N	4		
10		Effective Maintenance	Y/N	4		
11		Innovation Research	Y/N	3		
12	Societal Impact	Corporate Social Responsibility	Y/N	3		
13		Employee Satisfaction Index	Y/N	2		
14		Health and Safety	Y/N	3		
15		Green Transport	Y/N	2		
TOTAL SUSTAINABILITY SCORE				100		100



Journal Paper:

Lykou G., Mentzeloti D., Gritzalis D., "A new Methodology towards effectively assessing Data-Center sustainability", Computers & Security, Elsevier, January 2018.

Climate adaption: Addressing risks and impacts of climate change on Transport Sector

- Identify transport huge challenges posed by climate changes
- All transport sectors approach
- Detect and analyze global adaptation initiatives
- Focus on emerging adaptation challenges and opportunities in the transport sector
- Propose Measures to increase Transport Resilience

Adaptation Option Description	Effective Governance Measures categorized by :			Measure Type				Risk and Uncertainty	
	Green	Soft	Grey	No regrets	Low regrets	Win-win	Adaptive	Manag.	
Strategic planning of Sustainable transport development		X		X					
Create an Adaptation framework so as to engage stakeholders within the transport sector		X				X			
Incorporate Adaptation requirements into Legislation & Regulatory Norms		X			X				
Enhance Standards and National/ Regional Requirements		X			X				
Develop National Adaptation Strategy and Action Plan		X						X	
Require as prerequisite climate risk assessment and Environmental Assessment for the design of new plants to ensure integrity		X				X			
Ensure Funding for new infrastructure or existing infrastructure reinforcement				X				X	
Coordinate Infrastructure Future Planning		X				X			

Conference Paper:

Lykou G., Stergiopoulos G., Papachrysanthou A., Gritzalis D., **“Climate adaption: Addressing risks and impacts of climate change on Transport Sector”**, 11th Int. Confer. on Critical Infrastructure Protection (CIP-2017), USA, March 2017

Analysis and Classification of Adaptation Tools for Transport Sector Adaptation Planning

1. Scope & Organize

- Review climate change impacts
- Identify stakeholders and gain involvement
- Build working group
- Identify scope & planning area

4. Implement & Monitor

- Implement high priority actions
- Utilize plans to seek funding
- Track progress & evaluate effectiveness
- Assess new impacts information
- Revise strategies & priorities as needed

2. Access

- Refine impacts assessment & conduct asset inventory
- Conduct vulnerability assessment
- Conduct risk assessment
- Prioritize planning issues

3. Plan

- Establish vision & resiliency goals
- Identify & prioritize adaptation strategies
- Create action plan & schedule implementation

- Focus on climate-related adaptation planning for Transportation
- Classification of adaptation tools for adaptation assessment and risk planning
- A multi-faceted taxonomy
 - 1) Typology and target audience
 - 2) Climate impacts & sectors
 - 3) Adaptation planning steps
 - 4) Software tools according to functionality & mode of use
 - 5) Strengths and Weaknesses

➤ Measures for Adaptation Resilience & Risk management

Conference Paper:

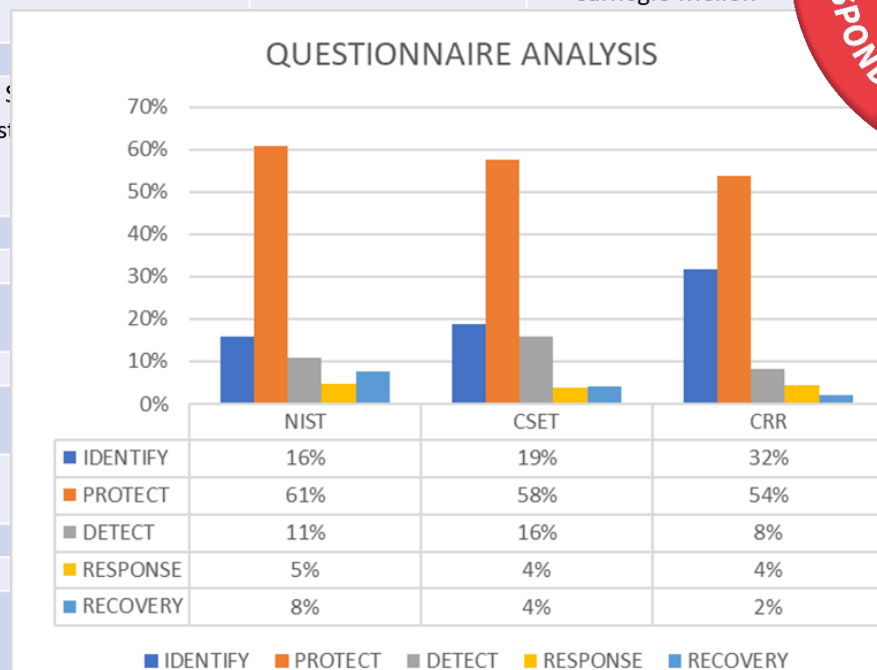
Lykou G., Stergiopoulos G., Papachrysanthou A., Gritzalis D., "Climate adaption: Addressing risks and impacts of climate change on Transport Sector", 11th Int. Confer. on Critical Infrastructure Protection (CIP-2017), USA, March 2017

CYBERSECURITY SELF-ASSESSMENT TOOLS: Securing Industrial Control Systems (ICS) in Critical Infrastructures

- Review and technical analysis of Self-Assessment tools for ICS (by CI operators)
- Content analysis for questionnaires & classification according to NIST Cybersecurity Framework



TOOL DESCRIPTION	CS ² SAT	CSET	SSAT	CRR
Type	Desktop software application tool	Desktop software application tool	Questionnaire XLS assisted Tool	Questionnaire PDF assisted Tool
Developer	Department of Energy National Laboratories	ICS-CERT / DHS	CPNI	US-CERT / DHS Carnegie Mellon
Origin	USA			
Description	Self-contained tool step-by-step process			
TOOL DESCRIPTION	CS ² SAT			
Step Process	6			
Survey Method	Structured Questionnaire			
Security Expertise Needed	YES			
Checks ICS Compliance with Security Standard	YES			
Database of industry available cyber-security practices	YES			
Sector average score	NO			
Recommendation List	YES			
Type of Result	Full Performance Evaluation			

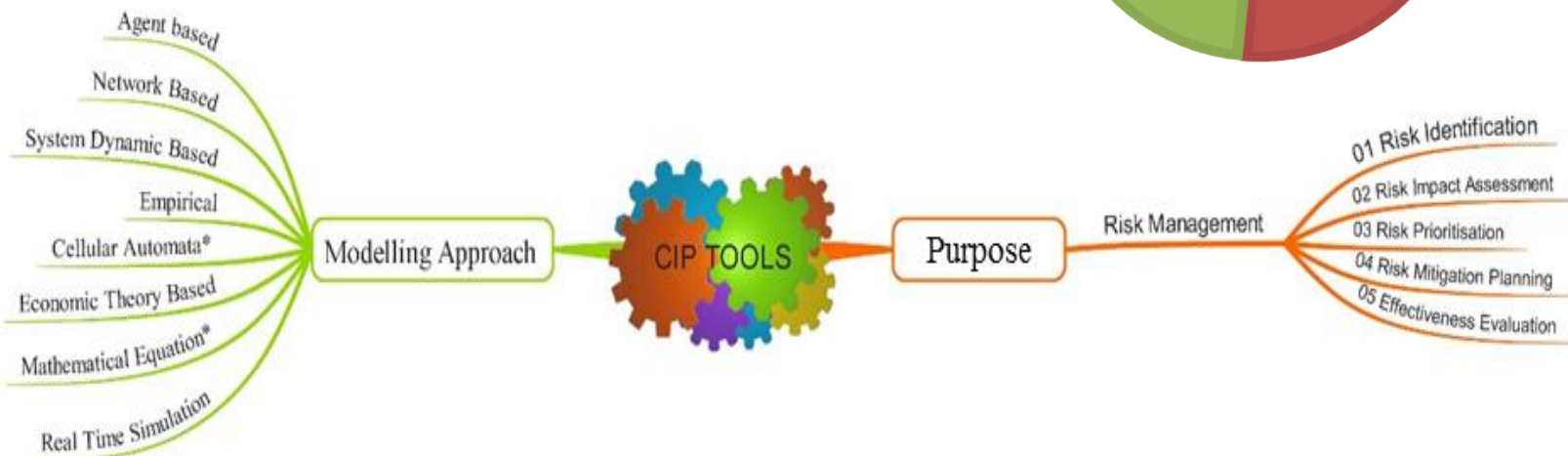
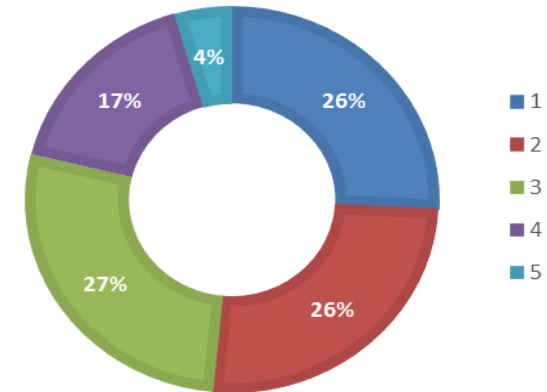


Lykou G., Anagnostopoulou A., Stergiopoulos G., Gritzalis D., "CYBERSECURITY SELF-ASSESSMENT TOOLS: Evaluating Importance for Securing Industrial Control Systems in Critical Infrastructures", in Proc. of the 13th Intern. Conference on Critical Information Infrastructures Security, CRITIS-2018, Kaunas, September 2018.

Critical Infrastructure Protection tools: Classification and comparison

- Technical Review and Comparison of 68 CIP tools, frameworks & methodologies
- Classification based on two aspects:
 - Technical modeling approach
 - Tool purpose and scope

CIP TOOLS QUANTITY OF RISK PURPOSE STAGES

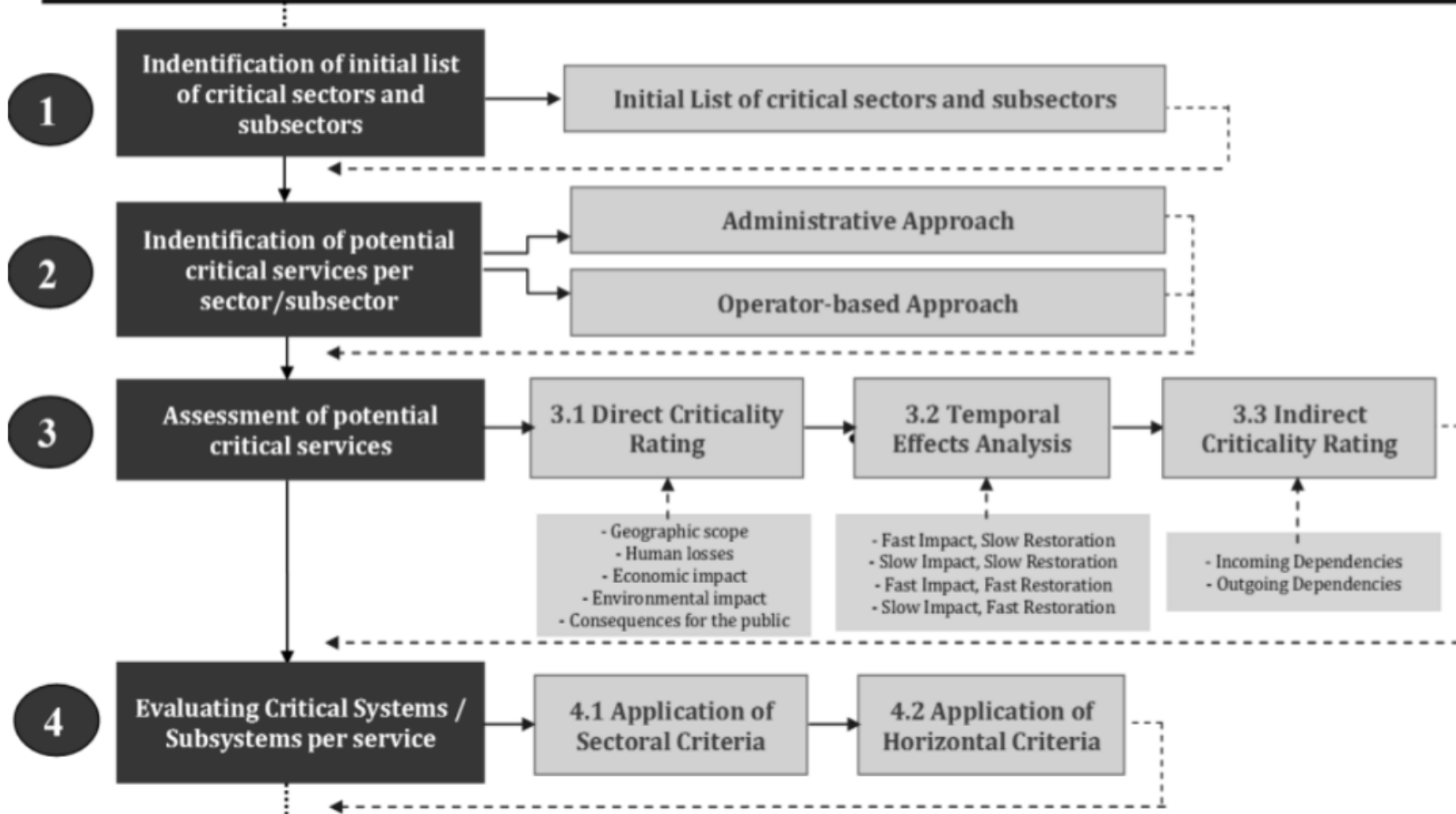


Conference Paper:

Stergiopoulos G., Vasilellis E., Lykou G., Kotzanikolaou P., Gritzalis D., “**Critical Infrastructure Protection Tools: Classification and Comparison**”, in Proc. of the 10th Inter. Conference on Critical Infrastructure Protection, USA, March 2016

Critical Infrastructure Protection: A Holistic Methodology for Greece

Implementation Methodology Guide of Critical Infrastructure Identification



-Journal Paper: Stergiopoulos G., Gritzalis D., Kotzanikolaou P., Magkos M., Lykou G., "*Holistic Protection of Critical Infrastructures*", Maritime Interdiction Operations Journal, Vol. 14, No. 1, pp. 29-41, September 2017

-Conference Paper: Gritzalis D., Stergiopoulos G., Kotzanikolaou P., Magkos E., Lykou G., "*Critical Infrastructure Protection: A Holistic Methodology for Greece*", in Proc. of the Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems (in conjunction with ESORICS-2016), Springer, Greece, September 2016

References

1. Lykou G., Anagnostopoulou A., Gritzalis D., "Smart Airports Cybersecurity: Threat Mitigation and Cyber Resilience", *Sensors*, January 2019.
2. Lykou G., Moustakas D., Gritzalis D., "Defending airports from UAS: A survey on cyber-attacks and counter-drone sensing technologies", *Sensors*, Vol. 20, No. 12, 2020.
3. Lykou G., Dedousis P., Stergiopoulos G., Gritzalis D., "Assessing Interdependencies and Congestion Delays in the Aviation Network", *IEEE Access*, December 2020.
4. Lykou G., Mentzeloti D., Gritzalis D., "A new methodology towards effectively assessing Data-Center sustainability", *Computers & Security*, 2018.
5. Lykou G., Iakovakis G., Gritzalis D., "Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management", in *Critical Infrastructure Security and Resilience*, Gritzalis, D., et al. (Eds.), pp. 245-260, Springer, 2019.
6. Lykou G., Anagnostopoulou A., Gritzalis D., "Implementing Cyber-Security Measures in Airports to Improve Cyber-Resilience", in *Proc. of the IEEE Global Internet of Things Summit*, pp. 305-310, Spain, 2018.
7. Lykou G., Anagnostopoulou A., Stergiopoulos, G., Gritzalis, D., "Cybersecurity self-assessment tools: Evaluating the importance of securing industrial control systems in Critical Infrastructures", in *Proc. of the 13th International Conference on Critical Information Infrastructures Security*, pp. 129-142, Springer, 2018.
8. Lykou G., Stergiopoulos G., Papachrysanthou A., Gritzalis D., "Climate adaption: Addressing risks and impacts of climate change on Transport Sector", in *Proc. of the 11th International Conference on Critical Infrastructure Protection*, USA, 2017.
9. Lykou G., Iakovakis G., Chronis G., Gritzalis D., "Analysis and Classification of Adaptation Tools for Transport Sector Adaptation Planning", in *Proc. of the 12th International Conference on Critical Information Infrastructures Security*, Springer, Italy, 2017.
10. Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-based critical infrastructure dependency analysis for large-scale and cross-sectoral failures", *International Journal of Critical Infrastructure Protection*, 2016.
11. Stergiopoulos G., Vasilellis E., Lykou G., Kotzanikolaou P., Gritzalis D., "Critical Infrastructure Protection tools: Classification and comparison", in *Proc. of the International Conference on Critical Infrastructure Protection*, Springer, USA, 2016.
12. Stergiopoulos G., Gritzalis D., Kotzanikolaou P., Magkos M., Lykou G., "Holistic Protection of Critical Infrastructures", *Maritime Interdiction Operations Journal*, Vol. 14, No. 1, pp. 29-41, 2017.
13. Gritzalis D., Stergiopoulos G., Kotzanikolaou P., Magkos E., Lykou G., "Critical Infrastructure Protection: A Holistic Methodology for Greece", in *Proc. of the Workshop on the Security of Industrial Control Systems and of Cyber-Physical Systems*, Springer, Greece, 2016.
14. Faily S., Lykou G., Partridge A., Gritzalis D., Mylonas A., Katos V., "Human-Centered Specification Exemplars for Critical Infrastructure Environments", in *Proc. of the 30th British Human-Computer Interaction Conference*, United Kingdom, 2016.
15. Theoharidou M., Kandias M., Gritzalis, D., "Securing transportation-critical infrastructures: Trends and perspectives", in *Proc. of the 7th IEEE Conference on Global Security, Safety and Sustainability*, pp. 171-178, Springer, 2012.
16. Dritsas S., Tsoumas B., Dritsou V., Konstantopoulos P., Gritzalis D., "OntoSPIT: SPIT Management through Ontologies", *Computer Communications*, vol. 32, no. 2, pp. 203-212, 2009.