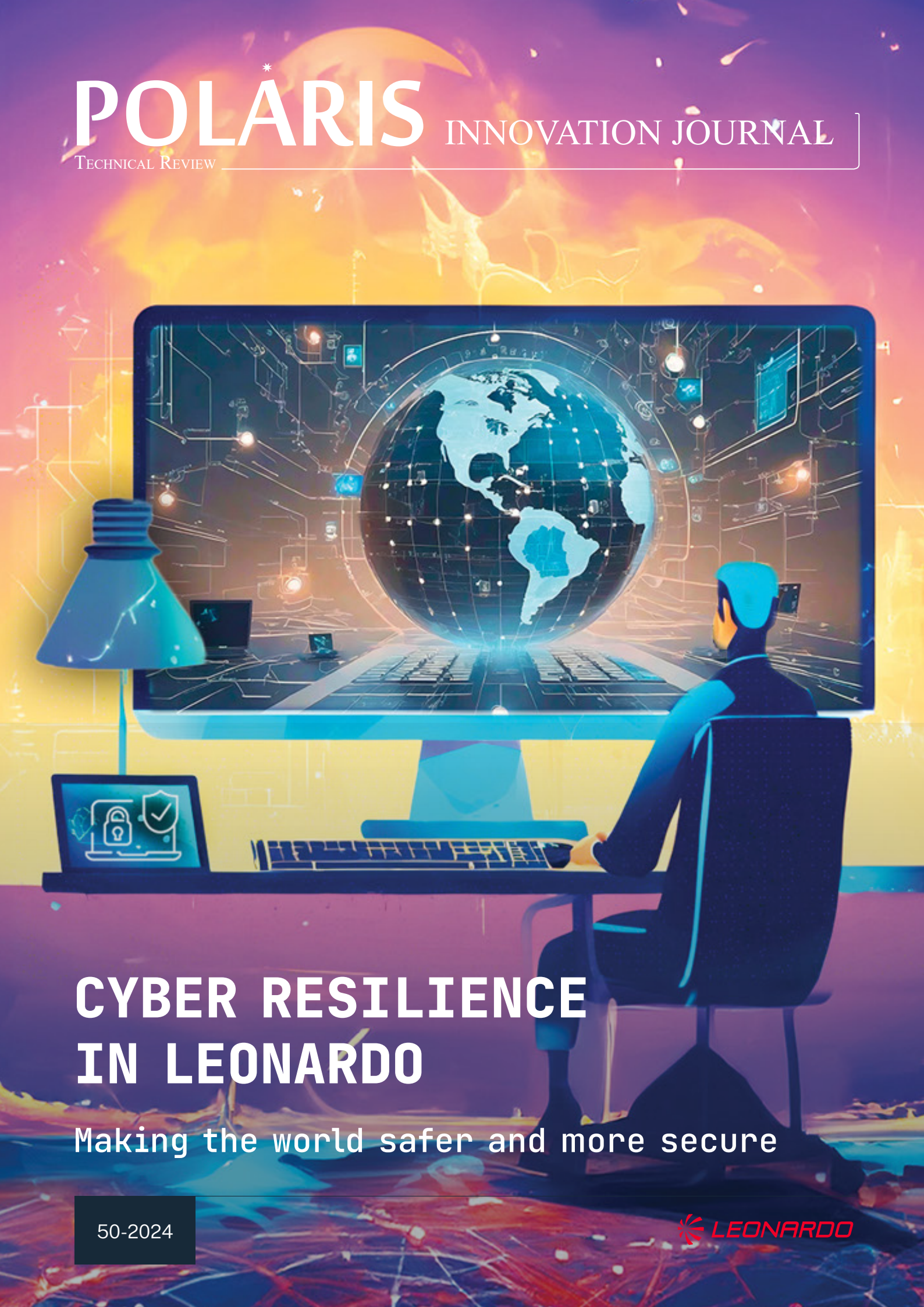
POLARIS
INNOVATION JOURNAL
TECHNICAL REVIEW



CYBER RESILIENCE IN LEONARDO

Making the world safer and more secure

50-2024

LEONARDO

PROPRIETARY NOTICE

contents

editorial

From shopping to work, from entertainment to sports and socialising, the digitisation of society has gone remarkably accelerating in the latest years. The recent pandemic has put a further irreversible push in this direction, by encouraging to migrate online many activities that were formerly performed in the presence. The amount of data exchanged throughout the network has greatly increased, as it now includes not only personal data but also data of those companies that have focused most on digitising their operational processes and services they provide, which furtherly increases their exposure to cyber attacks.
The same technologies that support digitisation also increase the incidence of cyber risk. It is a worrying paradox that pushes towards the development of new approaches to cope with cyber security attacks, which are getting more sophisticated, intense and frequent. Also, cyber attacks go evolving much faster than the countermeasures to deploy to face them. About such attacks, we just know they are to occur for sure, but it will become more and more difficult to understand when they will occur, as well as their origin, mode and type.

For these reasons, the approach based only on cyber security, which means to prevent the cyber threat from occurring, is not enough anymore. We believe it is necessary also to add a resilience-based approach. The term resilience derives from engineering of materials, to describe their property of resisting shocks by suffering just negligible damages that are temporary and reversible, but not any irrecoverable damage. When applied to the cyber threat, the term denotes the ability to manage it by using a prevention and reaction plan that allows to maintain essential levels of operation - albeit temporarily reduced - and to come back to full rate of activity in the shortest time. Cyber resilience is enabled by the design of a system in a way that first enables it withstanding and adapting to attacks or compromise of IT resources, and recovering from them, to go then focusing on rapid recovery of the attacked systems.
Cyber resilience approach is relevant to organisations, critical infrastructures, and public administration platforms, as it is based on identifying the critical areas of a system. This enables to evaluate their exposure at risks and to design and implement as proper those actions, that are relevant to manage the cyber threat and its seamless evolution over time.
Leonardo is a point of reference in the Security and Safety areas in general and has a leading position in these markets. Our company also has a recognised leadership in cyber security, due to its technological expertise and consolidated operational experience, it has acquired over its years of activity with customers of various types. Leonardo's systems protect both legacy and newly developed platforms and next-generation systems based on the 'cyber secure-by-design' approach, for national and international security, critical communications, aerospace, as well as for defence and fundamental services to citizens.

This issue of the POLARIS Innovation Journal is dedicated to cyber resilience and in particular to Leonardo's vision in this area. The articles illustrate (i) the cyber resilience methodologies defined by Leonardo within the framework of the guidelines issued at international level, (ii) the 'cyber secure-by-design' approach to making systems intrinsically reliable right from their design and development phase, (iii) the range of solutions designed by Leonardo to improve threat prevention. Making this framework even more challenging will be the spread of new disruptive technologies, including Artificial Intelligence, Big Data analytics, and Digital Twin, which for sure are to enable new threats but are also to provide new capabilities to counter them.
Enjoy reading and stay resilient!

Alessandro Massa
Product & Technology Innovation
Cyber & Security Solutions Division

Massimo Tedeschi
Engineering
Cyber & Security Solutions Division

Cyber Security & Resilience: to face Global Security Challenges in the Digital Era

Eleonora Cordaro[1], Ombretta Arvigo[1], Gabriele Bastianelli[2], Simona Sisto[1]

[1]Leonardo – Cyber & Security Solutions Division, [2]Leonardo - Corporate

The digital landscape of 2024 is marked by rapid technological advancements and geopolitical uncertainties, as highlighted by the 19th edition of the World Economic Forum (WEF) Global Risk Report. Notably, misinformation and cyberattacks emerge as significant perceived risks, reflecting the intricate interplay between technology and geopolitical tensions, further fuelled by advancements in high-impact technologies such as artificial intelligence. Our analysis delves into the way the market responds to such dynamic environment, with specific focus on key sectors for Leonardo, including Defence, Space, and Strategic Organization. These sectors are undergoing a paradigm shift as they intensify efforts to enhance cyber resilience and cybersecurity. Navigating the ever-changing cyber landscape poses challenges in predicting future threats, as the only certainty is the likelihood of encountering phenomena that are practically impossible to predict today. The imperative is to stay prepared to face these challenges by implementing adaptive cyber resilience strategies tailored to the demands of the digital era. This involves providing a comprehensive framework that empowers organizations to safeguard critical assets and maintain trust, in the face of unprecedented uncertainty.

CYBER THREATS LANDSCAPE, WHAT'S GOING ON?

Our world is intricately shaped by a confluence of rapid technological advancements and economic uncertainties, set against the backdrop of two formidable crises: climate and conflict.

The 19th edition of the World Economic Forum (WEF) Global Risk Report [1] paints a vivid picture of our society, where geopolitical tensions intertwine with active hostilities, while contributing to a global order that is marked by polarizing narratives, diminishing trust, and pervasive insecurity. This complex landscape fuels a growing sense of frustration with the prevailing status quo.

In the midst of this turbulence, the WEF Global Risks Perception Survey [2] reveals that two-thirds of respondents expect that the next decade will see the dominance of a multipolar order. As middle and great powers assert, enforce, and contest the existing rules and norms, the world becomes increasingly fragmented. Within such a segmented global order characterized by the lack of consensus and of international cooperation, the necessity for preparedness against emerging risks becomes paramount.

Such an environment leaves ample room for the escalation of risks, which are further pushed by unstoppable technological advancements, particularly in Artificial Intelligence. Within the intricate scenario depicted in Figure 1, the AI-generated misinformation and disinformation [3] (53% of respondents) and the cyberattacks (39% of respondents) rank among the top five risks that are expected to trigger a global crisis within 2024.

Looking forward over a two-years period, misinformation and disinformation are identified as the technological risks that feature the highest predicted impact (1st place), as well as cyber insecurity [4] (4th place - see Figure 2). The convergence of foreign and domestic actors that exploits misinformation to widen societal and political divides emerges as a critical concern, especially because of approximately three billion people who are expected to be involved in elections across multiple economies in the coming years.

The foresight into this future risk outlook is underpinned by a discernible surge in cybersecurity attacks that was observed since the latest half of 2022 to the earliest months of 2023, as it is outlined in the latest ENISA Threat Landscape Report [5]. The ongoing conflict, particularly the aggression against Ukraine, continues to exert a significant influence on shaping the cybersecurity environment. Hacktivism is experiencing consistent growth, marked by emerging novel factions, while ransomware groups demonstrate unprecedented spike and maintain a dominant position, as they represent more than 31% of the global threats.

Ransomware attacks have evolved with increasing sophistication, and adopt methods like double, triple and even quadruple extortion and supply chain attacks, to target organizations strategically. The emphasis on precision targeting, particularly in the industrial and manufacturing sectors, reveals a shift in tactics that are aimed at causing remarkable financial losses and operational downtime to high-value targets.

Simultaneously, the Distributed Denial of Service (DDoS) attacks persist as a constant threat that ranks the second position in terms of prevalence. The centrality of data is the foundation of modern Artificial Intelligence/Machine Learning (AI/ML) systems.

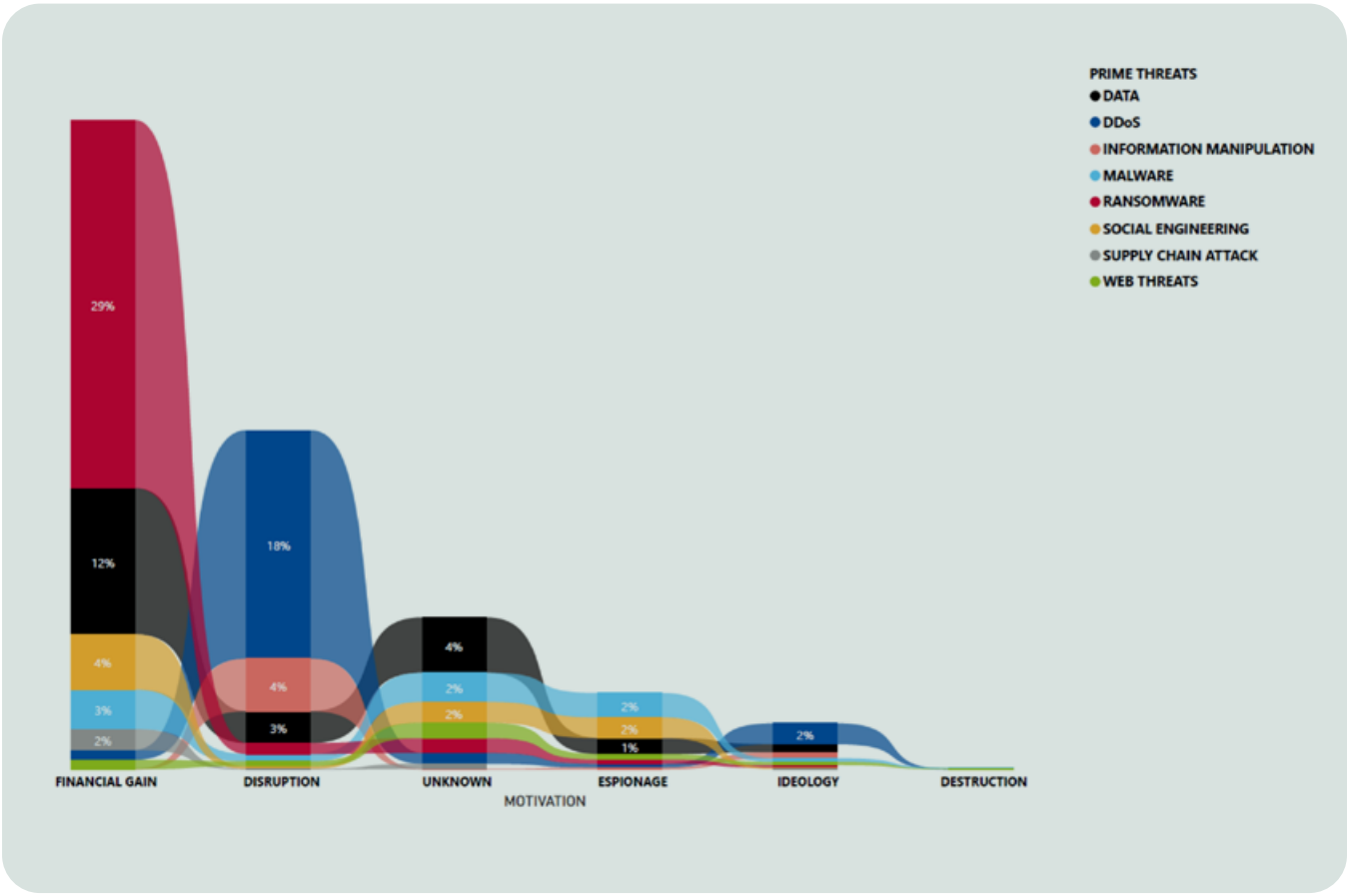
This places the data in the cloud-edge continuum as a major focal point for cybercriminals. Threats against data go ranging from blocking access to manipulating (e.g. poisoning) data, to disrupt the system behaviour. A detailed analysis of those threats, which also considers sectors and regions, reveals that public administrations, individuals, and healthcare sectors remain the primary targets for data leaks and breaches.

The majority of cases show that primary threats can be linked to one or more motivations, with some motivations that emerge as more prevalent than some others (Figure 3). Within the domain of ransomware attacks, while the primary motivation typically centres around financial gain, a small percentage of them involves disruptive motives, as well. Beyond financial gain, disruption is the second most common push, as more than 50% of those instances are attributed to various DDoS attacks.

As we delve into this multifaceted landscape, it becomes evident that the intertwining forces of geopolitics, technological acceleration, and evolving cyber threats shape the complex scenario we have to deal with, at the beginning of 2024.

1 – Current risk landscape – The top five risks that are believed the most likely to trigger a material crisis on global scale in 2024

2 – Future risk landscape – The global risks as ranked by severity, over the short and long term



3 – Motivation of Threat Actors per threat category (July 2022-June 2023)

A FOCUS ON THE CROSSOVER BETWEEN CYBERCRIME AND CYBERWARFARE

Building upon the intricate risk landscape we have outlined in the previous section, let's focus now on the evolving realm of cyber insecurity, pushed by the surge in cyberattacks. As we delve deeper into the multifaceted world of cyber threats, it becomes evident that cybercrime, defined by the UN Office on Drugs and Crime (UNODC) as an *"act that violates the law, which is perpetrated using ICTs to either target networks, systems, data, websites and/or technology or facilitate a crime"* [6], has undergone a transformative evolution.

As the digital threats raise, the cybercrime takes centre stage, as it is expanding its scope into a broad, multidimensional, and multi-domain paradigm. The recent Internet Organised Crime Threat Assessment (IOCTA) from EUROPOL [7] underscores the escalating menace that is posed to the European Union (EU) by the cybercrime. It also highlights that cybercriminals feature adaptability to emerging technologies, notably the Artificial Intelligence, while enhancing their cooperation and specialization.

This multidimensional threat landscape gains complexity, because of the convergence of Information Technology (IT), Operational Technology (OT), and Internet of Things (IoT) devices. The blurring of borders between cybersecurity and physical security, expands the attack surface and poses challenges to conventional defence mechanisms. The recent shift towards a more connected and interdependent world, further accentuates the challenges posed by cyber threats.

The interconnections among critical infrastructures amplifies the impact of cyberattacks beyond digital systems, thus necessitating a comprehensive and integrated approach to cybersecurity.

Moreover, the synergy between cybercrime and cyberwarfare, which is defined by the UNODC as the "*cyber acts that compromise and disrupt critical infrastructure systems that amount to an armed attack*" [8], is a phenomenon that has grown up in recent years. Tactics like ransomware and DDoS attacks, which are traditionally associated with cybercrime, now integrate with operations that target military domains and strategic assets, as elucidated by the Stockholm International Peace Research Institute (SIPRI)[9].

Ongoing geopolitical tensions, exemplified by the conflicts involving Russia, China, and the United States, bring these cyber trends into sharp relief. The war in Ukraine accentuates the intricate challenges faced by the European Union (EU), and confirms the surge in cyberattacks that go impacting critical infrastructure. As cyber incidents lead to warnings of "*unacceptable risks of spillover effects, misinterpretation, and possible escalation*" [10], the EU faces the imperative to redefine and expand the boundaries of its security landscape.

Beyond conventional defence, the holistic concept of national security now encompasses data production and use, cybersecurity, space control, infrastructure security, and energy resilience. Such an expanded perspective acknowledges the interconnected nature of modern threats, and emphasizes the need for a comprehensive and adaptive approach to safeguarding national interests.

THE MARKET RESPONSE

The ENISA Threat Landscape Report 2023 [5] provides detailed quantitative data that confirms the cybersecurity trends across various sectors. According to the report, ransomware remains the top threat, accounting for 34% of EU threats, with a noted increase in frequency and sophistication of attacks. Manufacturing (14%), health (13%), and public administration (11%) are the most targeted sectors by ransomware. Supply chain attacks have emerged as a significant concern, affecting 21% of public administration instances and showcasing the attackers' growing interest and capability in this domain. Data compromise has also seen an uptick in 2023, following a relatively stable 2022, with AI chatbots notably impacting the cybersecurity landscape.

DDoS attacks continue to present a persistent threat, being the second most prevalent in the EU. They are evolving to become larger, more complex, and increasingly targeting mobile networks and IoT devices. This trend highlights the critical importance of robust defense mechanisms in public administration, where 34% of DDoS attacks are directed, followed by the transport (17%) and banking/finance (9%) sectors.

In response to the evolving cyber threat landscape in 2024, significant market shifts are evident across five key sectors: public administration, healthcare, manufacturing, defence and Space.

In public administration, increased investments are dedicated to advanced cybersecurity infrastructures.

This includes the development of tailored cybersecurity solutions that emphasize data protection and threat intelligence, thus underscoring the need for operational integrity and public trust maintenance. The healthcare sector is also experiencing a similar trend, with a focus on safeguarding data of patients and medical services continuity. The market is adapting coherently, by offering specialized cybersecurity solutions, enhanced network security, and heightened awareness among healthcare professionals. The rise of cybersecurity insurance products is also notable, aiming to offset the financial risks associated with cyber incidents.

The manufacturing sector is adopting a dual approach: securing both the digital and the physical infrastructures. The integration of advanced cybersecurity measures like the real-time monitoring and the predictive analytics is becoming increasingly prevalent, alongside the adoption of secure-by-design principles that embed cybersecurity into the manufacturing process since its launch.

Meanwhile, in the Defence and Space sectors, the market response to cyber threats is evolving with a focus on resilience and adaptability. In Defence, a 'Secure by Design' strategy is paramount, as integrating DevSecOps (Development, Security, Operations) to ensure security is foundational in product development. This sector is also leveraging advanced Cyber Defence techniques, employing emerging disruptive technologies for proactive threat management. This approach is crucial for mission assurance and operational continuity in the face of unpredictable cyber challenges.

The Space sector is adopting 'Augmented Zero Trust' models that enhance information security across all operational levels and enable secure access to resources from any location. Here, the key focus is put on developing anti-fragile systems, which use AI to detect and neutralize threats in real-time, thereby thriving amid volatility and uncertainty.

Across all these sectors, the market response must be proactive, with growing emphasis put on AI and machine learning technologies for automated threat detection and response. This technological advancement is balanced with ethical considerations, especially regarding AI-generated misinformation.

In summary, the market's response to the 2024 cyber threat scenario is marked by heightened investments, sector-specific cybersecurity solutions, and by the integration of advanced technologies, which reflect an adaptive and dynamic approach to national security in the face of evolving cyber risks.

4 – Leonardo strategic sectors

Focus on 3 strategic areas for Leonardo: Defence, Space, National Strategic Organizations

In response to the intricate and evolving cyber threat landscape and to the market trends as discussed above, Leonardo stands at the forefront, strategically aligning its expertise to safeguard the three pivotal sectors for national security: Defence, Space, and National Strategic Organizations (Figure 4).

Leonardo provides Defence with a comprehensive approach that prioritizes data protection, integrity, and availability across mission-critical, multi-domain, and multi-dimension contexts. Leonardo's proprietary and structured approach to cyber resilience is central to achieve these objectives, as well as its cyber and multi-domain command and control solutions, and the Defence Cloud. The latter is an infrastructure that ensures distributed access to the resources necessary for conducting multi-domain operations and managing different levels of classification.

Leonardo also leverages its cyber and security capabilities to bolster the security and resilience of space assets in all the segments of the Space sector (ground segment, space segment, downstream services). Drawing on expertise spanning military and civil domains, the company has crafted a comprehensive ecosystem of solutions, services, and products. Leonardo's offerings cater to diverse domains within the Space sector, including Earth Observation, Navigation, Communications, and Security & Digital Awareness programs. Notably, the European Space Agency (ESA) has chosen Leonardo to design and operate its Cyber-Security Operations Centre (C-SOC) that contributes to the protection of European space assets from cyber threats.
Expanding its reach to National Strategic Organizations, Leonardo consistently engages with key stakeholders, such as Public Administrations, International Agencies, National Critical Infrastructures, and Police Forces.
This sector holds strategic significance for the National Security and the welfare of citizens.
Given the diverse nature of its participants, it features unique and specific security requirements for each stakeholder. Leveraging its experience and capabilities, Leonardo supports its customers in seizing the opportunities presented by the digital transition process and in facing present and future security challenges. For instance, at the national level Leonardo contributes to the secure digitalization of governmental bodies. This is exemplified by its pivotal role in delivering cybersecurity of the PSN (Polo Strategico Nazionale), the new cloud infrastructure for Public Administration aimed at ensuring higher-quality public services. Moreover, internationally, Leonardo has collaborated with DG Connect, the European Commission's directorate for digital policies, to develop the first pan-European virtual centre for real-time dynamic cyber risk management.
In such an extremely dynamic cyber terrain, Leonardo is dedicated to securing three strategic areas, ensuring safety, security, and resilience of our society. In an era where cyber threats continue to evolve, Leonardo's commitment to innovation, collaboration, and comprehensive defence remains unwavering.

WHAT'S NEXT?

As we navigate the complexities of the ever-evolving cyber landscape, one of the critical questions that rise up is: *how will the threat landscape evolve in the future, and how can Leonardo prepare for the resilience of its systems and those of its clients amid increasing complexity?*
Unfortunately, in the face of that escalating intricacy, predicting the risks we have to face and the threats we must protect against becomes a formidable challenge. For sure, encountering an increasing number of what Henry Bauer defines as "unknown unknowns" or Nassim Nicholas Taleb [11] refers to as "black swans" is becoming unavoidable.
In 1992, Bauer [12] categorized the "unknown" events in two different categories. "Known unknowns" are events that are challenging to predict and are potentially at high-impact, but can be explained basing on existing theoretical models and the current state of knowledge. In contrast, "unknown unknowns" are phenomena that cannot be interpreted by using existing models. This makes them impossible to predict, except through retrospective analysis, which is typical to the "black swans". Just as the belief that all swans are white is reinforced until a black swan is encountered.
Cyber resilience becomes paramount in handling the black swans posed by cyber threats, which are those unknown unknowns that organizations find challenging to predict and to defend against. Beyond the Cyber Security that addresses known unknowns, and the Information Security that manages known threats, the Cyber Resilience assumes a central role in fortifying against unforeseen and unpredictable challenges.
Recognizing the pivotal role of Cyber Resilience in our world, which is characterized by increasing structural fragility, Leonardo has accurately developed its own approach that is based on proprietary methodologies, processes, tools and products\solutions. These are natively integrated into every products of ours, and all phases of the life cycle of Leonardo's products, systems, and systems of systems are addressed in this way. This approach allows us to design, build and operate our systems, being always aware of the status of each system, sub-system and component from the cyber-security point of view and to intervene promptly whenever it were necessary. Our objective is to ensure the operational continuity of our customers, particularly in the Defence domain, where mission assurance is paramount. Leonardo's structured approach is anchored in the key concepts of *Secure By Design* and *Cyber Defence.* This entails employing Cyber Secure By Design methodologies, which are rooted in reference standards, to ascertain resilience requirements, design inherently secure systems, and employ DevSecOps for developing cyber-resilient products. Additionally, Cyber Defence involves delivering advanced services and solutions based on Emerging Disruptive Technologies to predict, prevent, detect, respond to - and recover from - advanced threats and systemic attacks. The effectiveness of the approach hinges on ensuring information security across

all operational levels, adopting a *zero-trust* logic, and empowering users to securely access resources from any location and device. In the pursuit of cyber resilience, Leonardo aims to transform unknown unknowns into known unknowns and shed light on unpredictable events.

Looking forward, Leonardo envisions the need to transcend the concept of resilience and to embrace the development of anti-fragile systems, i.e. systems that not only withstand stress, volatility, and disorder but also go thriving and improving while facing these challenges. These systems may leverage the evolution of current Emerging Disruptive Technologies, particularly the Artificial Intelligence, to detect anomalies in real-time and to neutralize threats through sophisticated hyper-automation techniques.
In such a dynamic environment, prioritizing preparation over prediction, investing in agile and flexible organizational structures, and embracing a multi-form, multi-domain, and multi-dimensional approach will be pivotal in securing a resilient and sustainable digital future. Leonardo is committed to continuing this journey, facing uncertainties and fortifying the foundations of cybersecurity, to meet the challenges that lie ahead.

Eleonora Cordaro: eleonora.cordaro@leonardo.com
Ombretta Arvigo: ombretta.arvigo@leonardo.com
Simona Sisto: simona.sisto@leonardo.com

REFERENCES

[1] The Global Risks Report 2024, 19th Edition - Insight Report https://www.weforum.org/publications/global-risks-report-2024/
[2] World Economic Forum Global Risks Perception Survey 2023-2024
[3] Persistent false information (deliberate or otherwise) widely spread through media networks, shifting public opinion in a significant way towards distrust in facts and authority. Includes, but is not limited to: false, imposter, manipulated and fabricated content
[4] Use of cyber weapons and tools to conduct cyberwarfare, cyberespionage and cybercrime to gain control over a digital presence and/or cause operational disruption. Includes: ransomware, data fraud or theft.
[5] 2023 ENISA Threat Landscape Report (ETL) https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023
[6] United Nations Office on Drugs and Crime (UNODC), 'Cybercrime in brief' https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html
[7] 2023 IOCTA https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN_0.pdf
[8] United Nations Office on Drugs and Crime (UNODC), 'Cyberwarfare' https://www.unodc.org/e4j/en/cybercrime/module-14/key-issues/cyberwarfare.html
[9] Cyber Crossover and Its Escalatory Risks for Europe, SIPRI Publications (September 2023) https://doi.org/10.55163/SIEP1930
[10] https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/
[11] N.N. Taleb, 2007 - The Black Swan: The Impact of the Highly Improbable, Random House.
[12] H.H. Bauer, 1992 - Scientific Literacy and the Myth of the Scientific Method. University of Illinois Press, Urbana and Chicago, (Illini Books edition, 1994).

Cyber Resilience: Ongoing Evolution of its Definition, Concept and Approach

Virginia Gugliotta[1], Alessio Caforio2, Paolo Di Serio[2], Emanuele Angelitti[1], Stefano Bordi[1], Gabriele Cicognani[1]

[1]Leonardo - Cyber & Security Solutions Division, [2]Leonardo – Corporate

Resilience is the ability of a system to withstand or to recover quickly from a disruption and continue to function. Cyber resilience is the ability of an organization to prepare for, respond to, and recover from cyber-attacks. Resilience is achieved through a combination of cybersecurity and business continuity management with deep integration of security, within the engineering processes at all stages of the life cycle. Cyber resilience requires a strategic governance to identify critical assets, assess risks, design and implement technical and procedural security control. This is needed to constantly measure effectiveness of the cyber resilience strategy and quickly react to any evolution of the threats. The Staff Education and Awareness on Cyber resilience is dedicated not only to cybersecurity experts/staff within an organisation, but potentially (and especially) also to any other staff. This holistic approach is required as a consequence of a wide, complex and diverse attack surface, where every activity of an organisation represents a possible vulnerability, with little to no exceptions, and therefore it needs to be integrated with an active role in the anticipation, defence and recovery strategy. By building cyber resilience, organizations can reduce the impact of cyber-attacks and maintain continuity of operation.

INTRODUCTION

The following article introduces and discusses the concept of cyber resilience. First, it considers resilience in the cyber context, therefore delving into the basic concept of resilience and cyber resilience and then underlining the differences between the latter and cyber security. The evolution of European legislation is then discussed through the introduction of the cyber resilience act and the mention of the current reference standards and frameworks regarding cyber resilience. At last, it goes into detail with Leonardo's posture on resilience, thus introducing a specific taxonomy and a guideline for a secure-by-design approach.

RESILIENCE IN CYBER CONTEXT

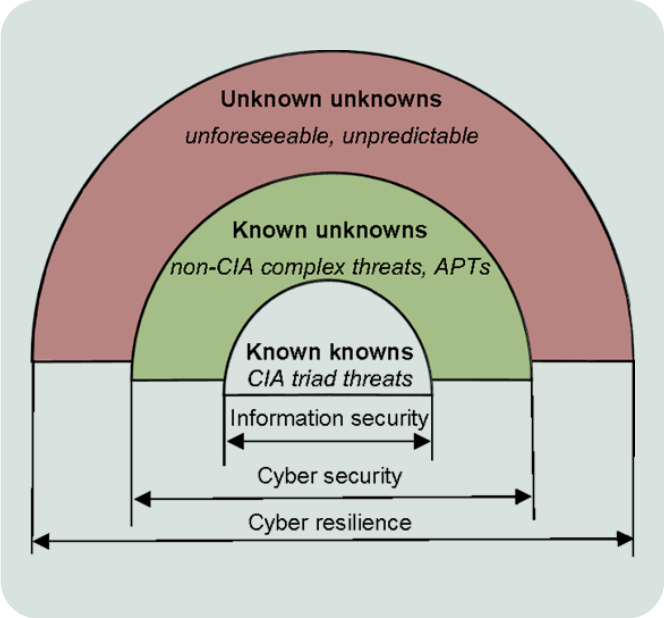
Resilience

Resilience is the ability to recover from difficult situations and to adapt to changes. It is a feature that can be developed and strengthened over time. In physics, the concept of resilience is closely related to the capacity of a system to recover from deformation without undergoing permanent changes. In particular, in case of collisions, resilience can refer to the ability of an object or a system to absorb the impact of that collision and then recover its original state or shape. Another example may be an elastic spring: resilience is associated with its ability to deform under an external force and then get back to its original shape when that force is not applied anymore. Generalizing, system resilience is the ability of a system to continue providing its required capabilities, despite

despite excessive stresses that can cause disruptions. It is an important quality attribute that ensures continuity of service, possibly under a degraded mode of operation, despite disturbances due to adverse events and conditions [1]. A resilient system must resist adversity and provide continuity of service, even when residual defects in the software or hardware cause the system to fail to correctly perform a required function or it fails to meet one or more of its quality requirements. The assets relevant to resilience include the system's component subsystems, hardware, software (e.g., applications, infrastructure, operating systems), the data the system stores, produces, and manipulates, and any other system-external assets. To ensure that systems are resilient, it is important to have a clear understanding of what resilience is and how it relates to other quality attributes such as availability, reliability, robustness, safety, security, and survivability.

Cyber resilience

In line with the cyber resilience act [2], cyber resilience is the ability of a system provided with digital element to maintain its functionality and to recover from cyber threats, such as cyber-attacks, data breaches, and other cyber related incidents. It focuses on the protection of sensitive data and of mission-critical infrastructure functionality, as well as the ability of organizations to respond quickly and effectively to adversaries and maintain continuity of their operations. In contrast to information security and cybersecurity, the aspect of cyber resilience can be distinctively visualized as shown in Figure 1 and understood as "the ability of a system, organization, mission, or business process to anticipate, withstand, recover from, and adapt to adversarial conditions, stresses, or attacks on the cyber resources it needs to function" [3]. Figure 1 shows information security (CIA triad), threats and response to them (i.e. known-knowns), cybersecurity (non-CIA triad, complex threats and ATPs) and corresponding responses to them (i.e. known-unknowns), and the wider cyber resilience, comprehensive of unforeseeable and unpredictable threats and responses to them (i.e. unknown-unknowns).



1 - Cyber resilience vs cybersecurity [4]

Cyber resilience

Unlike cybersecurity, cyber resilience is able to deliver business value, even in case of adverse cyber events, as its objective is business rather than information technology.

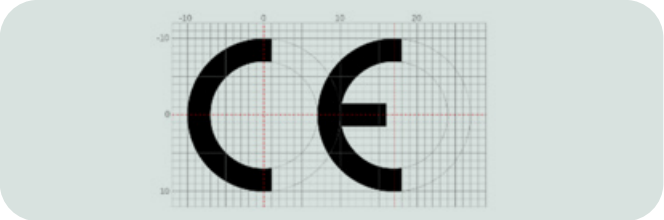
	Cyber resilience	Cybersecurity
Objective	Ensure business delivery	Protect IT systems
Intention	Safe-to-fail	Fail-safe
Approach	Build security from within	Apply security from the outside
Architecture	Multi layered protection	Single layered protection
Scope	Holistic, network of organizations	Atomistic, one organization

Table 1 - Aspects of cyber resilience and cybersecurity [5]

From the security perspective, in cybersecurity a system has to be fail-safe, which means that the system should be running as usual and be able to withstand cyber events. In addition to this, resilient systems must be able to fail in a controlled way. In the cyber resilience approach, security needs to be build-in rather than being an add-on. The architecture of resilient systems should be especially suited for the recovery of each layer, in order to allow for partial failure, according to the requirement of safe-to-fail. The architecture of cybersecurity consists just of a hard outer protective shell. In the end, cyber resilient analysis cannot consider only a single system that is suitable both for the multitude of system's interconnections and for their strength in terms of capability to recover from adverse events [5]. The following Table 1 summarizes the concepts discussed above that distinguish cyber resilience and cybersecurity in terms of objectives, intentions, approaches, architectures and scopes.

THE EVOLUTION OF EUROPEAN LEGISLATION: THE CYBER RESILIENCE ACT

While some products with digital elements fall under existing internal market legislation, most of the hardware and software products are currently not covered by any EU legislation addressing their cybersecurity, even if the rising frequency of cybersecurity attacks is causing substantial societal and economic costs.
The cyber resilience act (CRA) [2], is a legislative proposal that establishes the mandatory IT security requirements for CE marking (Figure 2) for all the network-connected products placed on the EU market.



2 – The CE marking

Its objectives are:
- Guarantee that the HW and SW products connected to the network and placed on the European market are secure, and security updates and correct information are ensured to users throughout the entire product life cycle;
- Identify a new legislative framework to verify compliance for HW and SW manufacturers: this framework has to be coherent with the currently existing one, referred to the Common Criteria model.

The products to which it applies are:
- Hardware products and components placed on the market separately (laptops, smart appliances, mobile phones, network equipment for CPUs);
- Software products and components placed on the market separately (operating systems, word processors, games or mobile apps);
- Other products with digital elements, coupled with corresponding data processing solutions intended for the EU market, included equipment subject to the RED – Radio Equipment Directive.

It doesn't apply to:
- Products already sold and in use;
- Products subject to specific regulations (medical devices, motor vehicles, civil aviation);
- Products for military or national security use only;
- Cloud/SaaS services already covered by the NIS2 Directive (except for remote data processing essential for the functionality of the product);
- Free open-source software (if not intended for commercial use).

The CRA aims to increase awareness of the critical role of cybersecurity in all aspects of a product's life cycle. In line with this objective, let's explore the obligations of manufacturers.
As shown in Figure 3, during the design and development phase are expected:
- Assessment of the risks associated with a product;
- A framework with essential product requirements (technical), process requirements (management) and transparency towards the users (documentation);
- Certification: verification of compliance with rigid requirements depending on criticality of the products (to be repeated in case of significant logical or physical changes).

In the maintenance phase are expected:
- Continuous vulnerability management with periodic testing and patch distribution for 5 years;
- Sharing of information related to vulnerabilities and incidents;
- Documentation of all elements useful for understanding risks and their mitigation.

To understand which conformity assessment they must follow, the products are categorized according to their level of risk, as shown in Figure 4:
- *Default category:* non-critical products for which only self-assessed conformity is required;
- *Critical "Class I":* products for which the manufacturer can carry out conformity assessment under his own responsibility, by declaring he has followed precise market standards, security specifications or cyber security certifications already required by EU;
- *Critical "Class II":* products at higher risk, for which a third party is involved in their conformity assessment;
- *Highly critical:* products with mandatory EU certification.

As anticipated, the products must satisfy the following requirements:

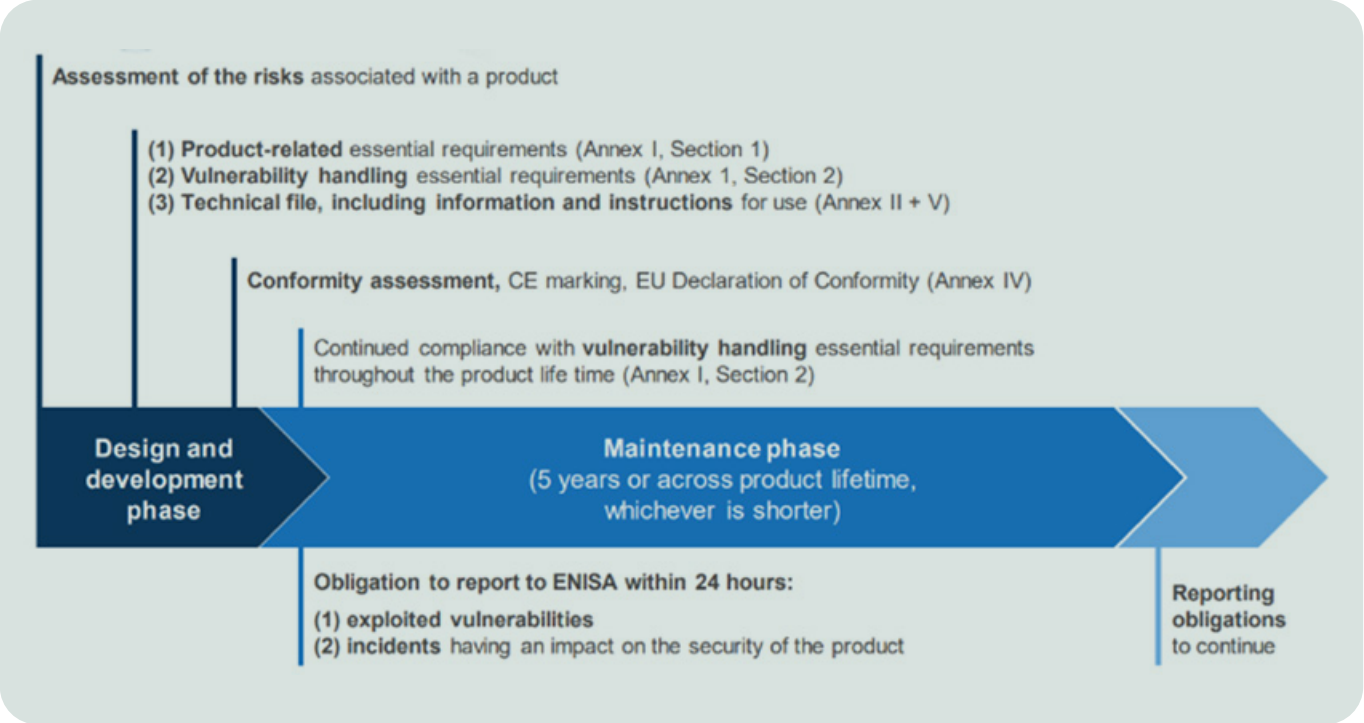
Product-related essential requirements (e.g. appropriate level of security, sale without vulnerabilities, risk analysis);

Process requirements (e.g. identification and documentation of dependencies and vulnerabilities, patching, tests and reviews, coordinated vulnerability disclosure policy);

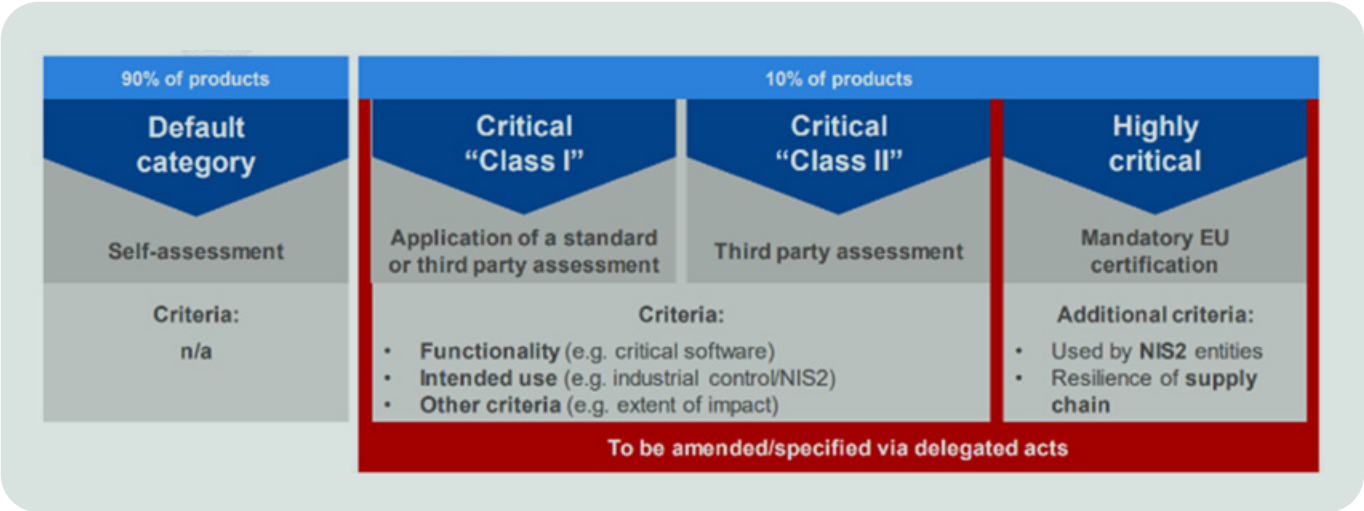
Transparency and information (e.g. CE marking, SBOM, EU Declaration of conformity, intended use, instructions for secure use and data deletion).

It's necessary to ensure that the CRA must be harmonized with the already existing regulations/legislations at European level (GDPR, cybersecurity act, Digital service act, NIS2 Directive), in order to avoid unnecessary duplication of flows and product assessments/certifications.

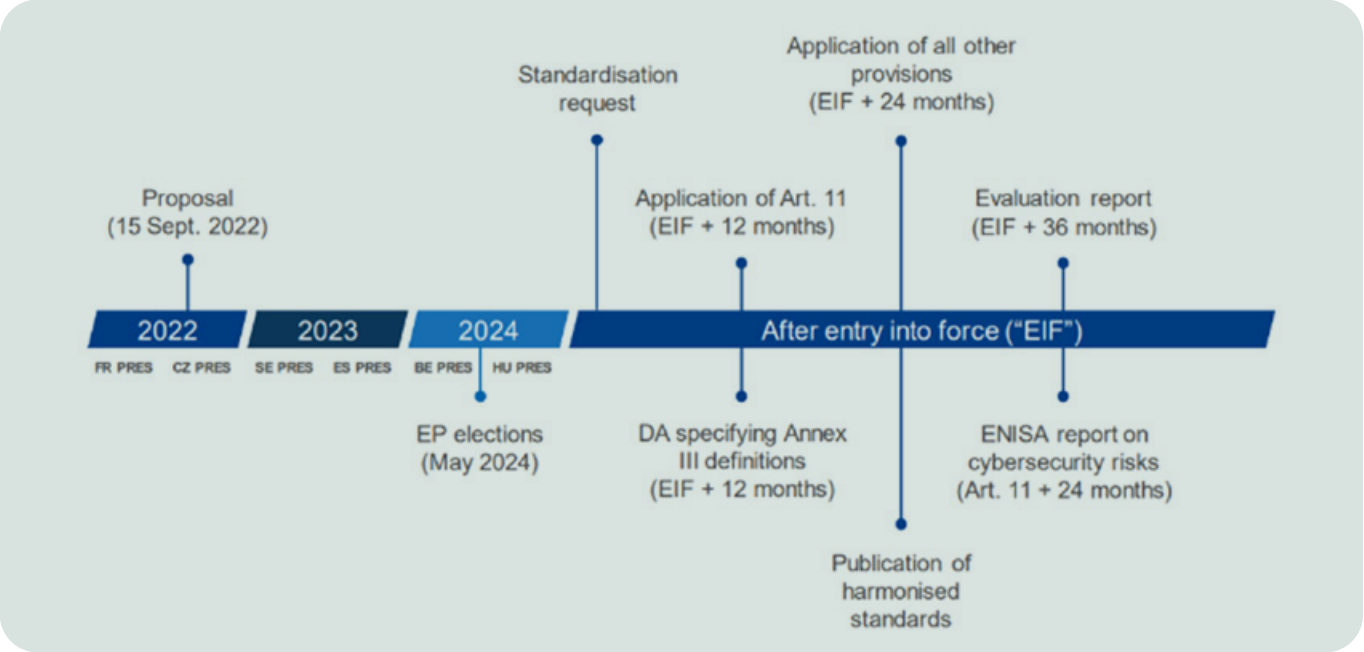
As shown in Figure 5, the CRA is scheduled to become operative in 2026, which underscores the necessity to plan the comprehensive assessment and validation of the Division's products and of the activities needed for certification as soon as possible. This proactive approach is crucial to prevent from market disruptions and potential block of our products on the market. To obtain such product certification it's necessary to set up a secure-by-design framework and the initial risk assessment, but also to guarantee the resilience management.



3 – Obligations of manufacturers



4 – Conformity assessment

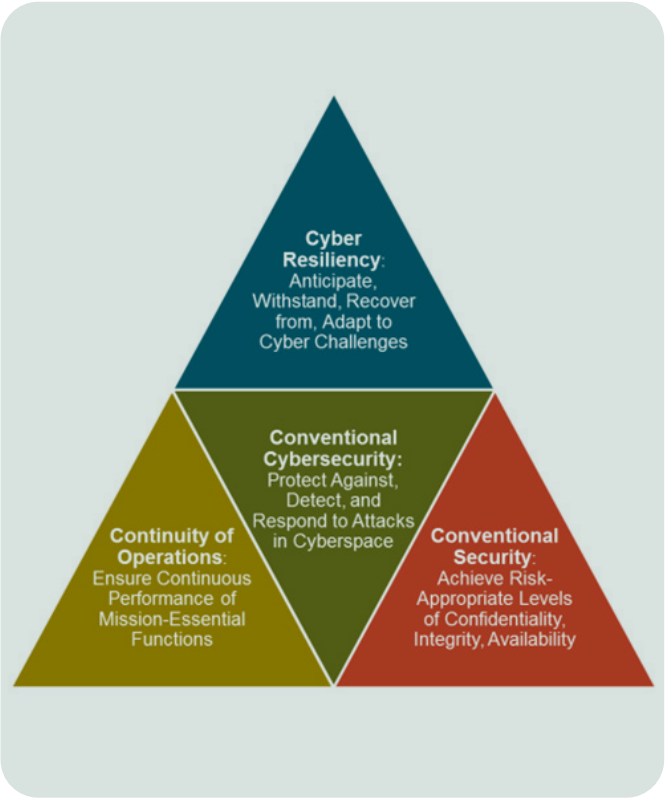


5 – Tentative CRA timeline

RELEVANT STANDARDS AND FRAMEWORKS

While standards related to security exist and have been evolving since decades, the standards associated to cyber resilience have been almost recently published. Such standards have introduced innovative concepts for the Security Communities and some of them have become the foundations of applicable regulations in many Countries. The same standards define the continuity of operations, the conventional cybersecurity, and the conventional security practices as the basis of cyber resilience, as shown in Figure 6. To establish a resilient ecosystem, they must be implemented as integrated layers, to ensure adaptability and perseverance in the ever-evolving digital landscape.

The following paragraphs outline some standards issued by two of the most important international organizations, such as the National Institute of Standards and Technology (NIST) [7] and the MITRE [8]. The NIST is a United States government laboratory that develops, tests, and recommends the best practices for Federal Agencies and other organizations related to aspects such as the online security. Metrics, measurements, and regulations are stated by the NIST to help strengthen the reliability and security of technologies being developed. The MITRE is an American not-for-profit organization that operates in the public interest in various field like the IT security.



6 - Foundations of cyber resilience [6]

NIST 800-160v1r1: Engineering Trustworthy Secure Systems

NIST SP 800-160 Vol. 1 Rev. 1 Engineering Trustworthy Secure Systems (NIST 800-160v1r1) [9] fixes the key points to develop a secure system engineering. This publication:

- provides the basis for establishing a discipline for system security engineering as a part of the engineering trustworthy secure system in terms of its principles, concepts, activities, and tasks;
- provides compelling evidence to support claims that meet its requirements;
- enables the delivery of the required system capability despite every form of adversity;
- enforces constraints to ensure that only the desired behaviours and outcomes are realized;
- fosters a common mindset to deliver security for any system;
- demonstrates how the selected systems security engineering principles, concepts, activities, and tasks can be effectively applied to systems engineering activities advances the field of systems security engineering;
- serves as a basis for the development of educational and training programs.

This publication also describes security design principles, concepts and techniques that can be applied in case of:

- modification, evolution and decommissioning of an existing capability or system;
- development of a new capability or system;
- development of a dedicated, domain-specific, or special-purpose capability or system, or of a system of systems.

NIST 800-160v2r1: Developing Cyber-Resilient Systems

The publication "NIST SP 800-160 Vol. 2 Rev. 1 Developing Cyber-Resilient Systems: A Systems Security Engineering Approach (NIST 800-160v2r1)" [10] is aimed to provide a framework that helps understanding and applying cyber resilience in the systems security engineering and risk management.

The systems it involves are:

- general-purpose or multi-use systems, shared services or common infrastructures;
- dedicated or special-purpose systems, large-scale processing environments, cyber-physical systems, Internet of Things or Network of Things devices, systems of systems.

Cyber resilience goals, objectives, techniques, approaches and design principles provide automatic responses - or support responses from cyber defenders - to detected indicators of a possible or suspected adversity or to warnings of potential forthcoming adverse conditions. A cyber resilience analysis is performed in order to support engineering and risk management decisions, as well as to enable the system to meet its mission assurance, business continuity or other security requirements.

CYBER RESILIENCE IN LEONARDO

Leonardo is active part in defining the posture about resilience, both by collaborating with organizations and institutions and by defining the necessary obligations in its processes. Within the AIAD (the community of Italian Defence Industries), Leonardo contributes defining a taxonomy or "operational pillars" of everything concerning cyber. Inwardly, Leonardo has issued a Directive on "Cyber resilience in the life cycle of products and services" [11], in which the cyber resilience principles and processes for security development and maintenance are defined.
Leonardo adopts the definition of cyber resilience by NIST [10]: "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources".
Objectives of cyber resilience are wider than confidentiality, integrity and availability of information or of system services.

Cyber resilience includes also objectives like design integrity, viability of mission functions, limited damage, etc.; then, it is applicable to a larger set of systems and use cases, in order to face more and more new and complex cyber threats.
In Leonardo, cyber resilience is founded on the application of the security-by-design principle and of systems security engineering discipline to products (and services) developed for customers. This is in line with the objectives expressed in the Cyber Resilience Act proposal of European Union [2], which bolsters cybersecurity rules to ensure more secure hardware and software products.
Of course, the cyber resilience of products is different from the cyber security of IT infrastructures but it benefits from that. Indeed, the cyber resilience of a product is supported by the cybersecurity capabilities provided by the IT infrastructure within which products are deployed.

However, it might be dangerous to think (and to rely on such an idea) that a generic customer enterprise IT infrastructure could completely counter all the threats specific to products, to achieve the cyber resilience objectives.
A product is cyber resilient if it is provided with "integrated" security measures as a fundamental part of its architecture, by applying the cyber resilience principles and processes as defined in the Leonardo Directive on "Cyber resilience in the life cycle of products and services" [11] mentioned above.
Indeed, cyber resilience solutions for complex products (e.g. system of systems) are developed (as outlined in the Directive) by applying and governing an interdisciplinary approach that should integrate and combine technologies, policies, procedures, standards, regulations, staff skills, organization. This approach is mainly driven by:

- understanding the context in which the product is supposed to go operating, in order to understand its scope, the associated threat scenarios and threat capabilities (with respect to the specific attack surface);
- stakeholders' security needs, in terms of security risk appetite, security objectives/requirements, business constraints;
- the applicable internal and external security standards, regulations, and their overlap with other disciplines (e.g. safety);
- the Leonardo internal security engineering guidelines, practices, processes, and resources;
- the applicable security certification/accreditation processes.

According to the Leonardo Directive and under the governance of the Corporate central function of the Company for product cyber resilience, the Leonardo Divisions are identifying and appointing their qualified personnel to manage and implement the product cyber resilience of their products.

The Product Cyber Resilient Officers (PCRO) coordinate cyber resilience activities at divisional level.
The Product Cyber Resilience Managers (PCRM) report to PCRO and manage cyber resilience activities for the entire product life cycle, up to delivery to customer and the subsequent maintenance, use and decommissioning.

The PCRO and PCRM are supported by cybersecurity specialists for all the technical activities.
In conclusion, it is important to highlight how the implementation of cyber resilience into Leonardo products is a technical and organizational process with continuous improvements, aimed at addressing both explicit and implicit customer requirements, to deliver products that are secure and resilient to cyber-attacks along their entire life cycle.

A taxonomy for cyber resilience

Defining a detailed taxonomy of cyber resilience is useful for several reasons, among which the provision of a structured way to categorize and organize elements and concepts related to cyber resilience. This ensures that everyone involved understands and communicates using the same terms, thus establishing a common language and framework for discussing about cyber resilience issues. This taxonomy is based on analysis of norms, standards and publications of the NIST and the NATO that are used in the fields in which Leonardo operates. It's a flexible tool, rather than a rigid set of rules, which is tailored to meet the evolving standard needs and is meant to adapt or eventually expand to accommodate new perspectives or changes in the context. Thus, it's always subject to updates and evolutions/improvements.

Such an ongoing process ensures that the taxonomy remains aligned with the current state of standards within a given domain, preventing it from becoming inadequate or obsolete.

As explained above, the three pillars that are governed by Cyber Resilience are the continuity of operations, the conventional cybersecurity, and the conventional security practices. This taxonomy encompasses these three elements and adds explicitly more specific resilience activities, such as cyber resilience engineering and simulation & training.

These two activities are not anymore a part of security or continuity practices, but are approached and conducted with a central, transversal, and holistic vision and a comprehensive perspective, and are therefore placed on the same level as the others.

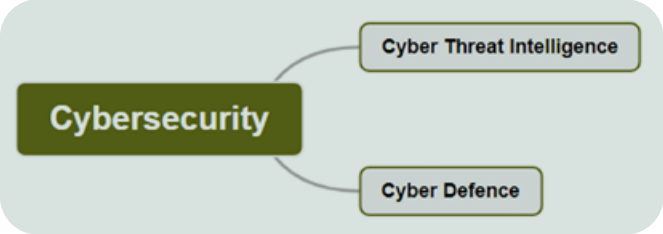
As shown in Figure 7, cyber resilience encompasses (inter) connected key elements, each playing a crucial role:

- cyber resilience engineering;
- cybersecurity;
- conventional security;
- simulation & training;
- business continuity/mission assurance.

7 – First level elements of cyber resilience

The two essential pillars of cybersecurity (Figure 8) are:

- *cyber threat intelligence:* it involves preventive techniques;
- *cyber defence:* the means to achieve and execute defensive measures to counter cyber threats.



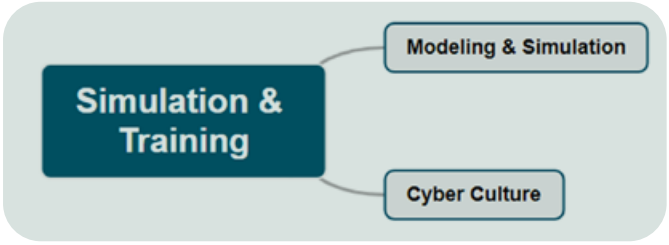
8 – Elements of cybersecurity

The elements of conventional security linked to cyber resilience, as shown in Figure 9, are: communication security, information assurance and information security and CIS security, which are both part of information assurance together with personnel, physical and industrial security, according to NATO Primary Directive on Information Management [12].

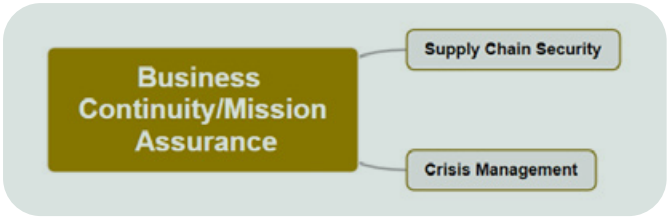
9 – Elements of conventional security

As shown in Figure 10, Simulation & Training consists of modelling & simulation that includes activities like wargaming as part of the cyberspace operations, and of a robust cyber culture. These components form a comprehensive approach to cyber resilience, in which personnel actively contribute to evolve and maintain the resilience in the face of evolving cyber challenges.

The supply chain security and the crisis management are integral components within the broader concepts of Business Continuity and Mission Assurance, as shown in Figure 11.

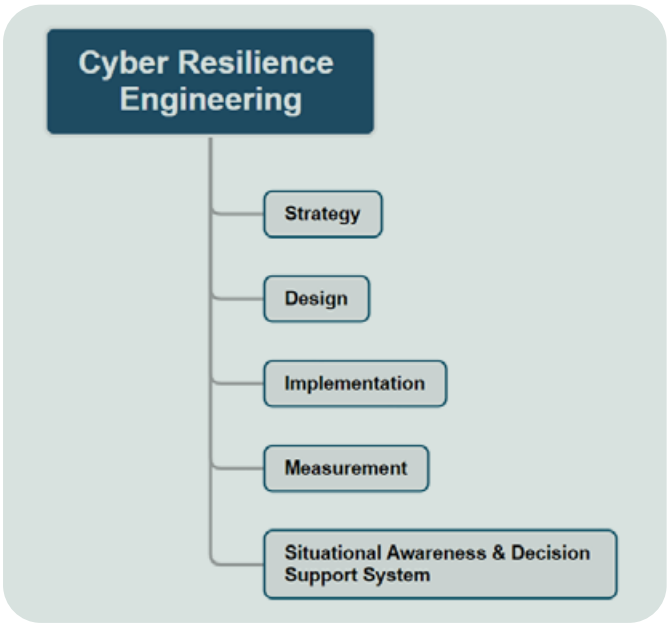


10 – Elements of simulation & training



11 – Elements of business continuity/mission assurance

Starting from the NIST 800-160 Vol.2 Rev.1 [10], cyber resilience engineering's constructs, as shown in Figure 12, can be included in-and reflected on-five main pillars as *strategy, design, implementation, measurement and situational awareness & decision support system.*
By continuously updating and refining the taxonomy based on new insights and experiences, Leonardo is able to improve its cyber resilience strategies over time. In fact, in an era where digital interconnectedness prevails, the strength of cyber resilience is a necessity, rather than just a choice.



12 – Elements of cyber resilience engineering

Cyber resilience engineering

According to the NIST 800-160 Vol.2 Rev.1 [10], the cyber resilience engineering is "*a comprehensive approach to enhancing an organization's ability to anticipate, withstand, adapt to, and recover from cyber threats and disruptions. It encompasses a wide range of strategies, practices, and technologies that aim to build an organization's resilience to cyber threats across the entire IT infrastructure*".
As mentioned in the taxonomy above, the first pillar of cyber resilience engineering is *strategy* that includes:

- *threat modeling & assessment* (e.g. business impact analysis, mission assurance analysis);
- *standard & compliance*: integral to a robust cyber resilience strategy;
- *risk management*: to address how the organization intends to assess, respond to and monitor risks;
- *goals & objectives*: used respectively to express high-level stakeholder concerns and priorities, and in scoring methods and summaries of analyses (e.g. cyber resilience posture assessments).

The core of the *design* pillar is formed by terse statements that describe how key concepts do apply to the system design throughout the system life cycle:

- *strategic design principles*: to guide and inform engineering analysis and risk analysis;
- *structural design principles*: to guide and inform the implementation decisions and approaches;
- *system security architecture*: that conveys information about how the system is partitioned into security domains and makes use of security-relevant elements to enforce security policies.

Implementation is precisely the third pillar and includes:

- *solutions* to provide a sufficient level of cyber resilience to meet stakeholder needs and reduce risks to mission or business capabilities in case of advanced persistent threats;
- *techniques* to characterize technologies, processes, or practices, providing capabilities to achieve one or more cyber resilience objectives;
- *mitigation* to reduce the level of risk associated with one or more threat events or threat scenarios;
- *integration* to synthesize a set of system elements into a realized system that satisfies the system requirements.

The *measurement* encompasses the technical processes of:

- *verification* to provide objective evidence that the system fulfils its specified requirements and characteristics;
- *validation* to provide objective evidence that the system fulfils its business or mission objectives and stakeholder requirements, achieving its intended use in its intended operational environment;
- *3rd party assurance*;
- *monitoring* that the system is operating in a secure manner and is compliant with regulations, procedures and directives.

Situational awareness & decision support system is the last pillar. Situational awareness represents the capability that enables the visibility of what is happening in the cyber domain for effective decision-making.

Guideline for "Cyber resilience by design"

The Cyber resilience correct implementation must be based on application of the security-by-design principle: security measures must be built in systems, by applying practices of systems security engineering and of its speciality - the cyber resilience engineering - right since the system conception phase.
In order to better clarify such approach and to show how the security problem of countering cyber-threats can be addressed since the very beginning, it is useful to outline a high-level engineering process in terms of main tasks and, for each one, of the needed main cyber resilience activities:

1. **Mission goals and business opportunities analysis and Context characterization:**
   a. *security strategy definition to protect business and mission*
   b. *security objectives definition*
2. **Architecture definition and requirements development:**
   a. *preliminary Security Risk Assessment (SRA)*
   b. *definition of security measures and architecture*
   c. *definition of the security requirements*
3. **System Design:**
   a. *assignment of security requirements to system elements*
   b. *detailed design of security mechanisms*
   c. *refinement of the architecture*
   d. *updated SRA based on model refinement, better definition of the attack surface and inclusion of third parties' components (Supply Chain Security)*

4. **System Implementation:**
   a. *implementation of security mechanisms through in-house development or acquisition from third parties or reuse of security building blocks already available*
   b. *updated SRA based on model refinement and better definition of the attack surface*
5. **Verification of absence of implementation errors:**
   a. *use of security testing tools for writing secure source code (e.g. applying DevSecOps approach)*
   b. *use of security tools and processes to verify the reliability of parts supplied by external suppliers*
6. **System elements verification:**
   a. *test to verify that the security requirements are correctly implemented at the level of single system element*
   b. *vulnerability tests on each single element*
   c. *remediation vulnerability and subsequent updating of SRA*
7. **Integration of system elements:**
   a. *test to verify that security requirements are correctly implemented at system level*
   b. *system-level vulnerability testing*
   c. *remediation of vulnerabilities found and subsequent updating of SRA*
8. **System Validation testing:**
   a. *validation tests of security solutions against the customer's security objectives expected for the operating environment*
   b. *vulnerability tests and penetration tests to validate the security posture in operational environment*
   c. *remediation of vulnerability and subsequent updating of SRA*
9. **Deployment, Maintenance, Disposal:**
   a. *assessments and management of changes due to commissioning or decommissioning with respect to the security objectives defined with the customer*
   b. *monitoring the correct functioning of the security mechanisms and management of any anomaly*
   c. *monitoring to find out new applicable threats*
   d. *monitoring and management of new vulnerabilities of ad hoc developed modules and third-party components integrated into the system*
   e. *monitoring security incidents involving the system and evaluating design improvements*
   f. *update of SRA, based on changes in risk factors (e.g.: new threats, new vulnerabilities, frequency of incidents, etc.), system characteristics and risk criteria / appetite.*

It is important to remark that cyber resilience activities can be grouped and performed sequentially or iteratively, according to the level of decomposition of the system, to the approaches to project management (e.g. waterfall or agile) and to the project events that occurred.

CONCLUSIONS

The concept of resilience questions the approach to cyber security, extending it towards mission assurance and business continuity, while entirely readdressing it towards the proactive coexistence with cyber threats. It is done by reviewing and reformatting business processes and cyber culture towards this new perspective, and by introducing new complementary processes and technologies. In fact, to foster this coexistence, organizations must adopt specific strategies and measures that regard not only the integration of advanced technologies, but also human and procedural elements that constitute the cybersecurity posture.

A critical aspect is the cultivation of a cyber culture, as well as the continuous training and awareness programs, to empower the knowledge and skills required to identify and respond effectively to potential cyber threats. At the same time, it's essential to introduce new corresponding tailored processes that align with the evolving threat landscape.

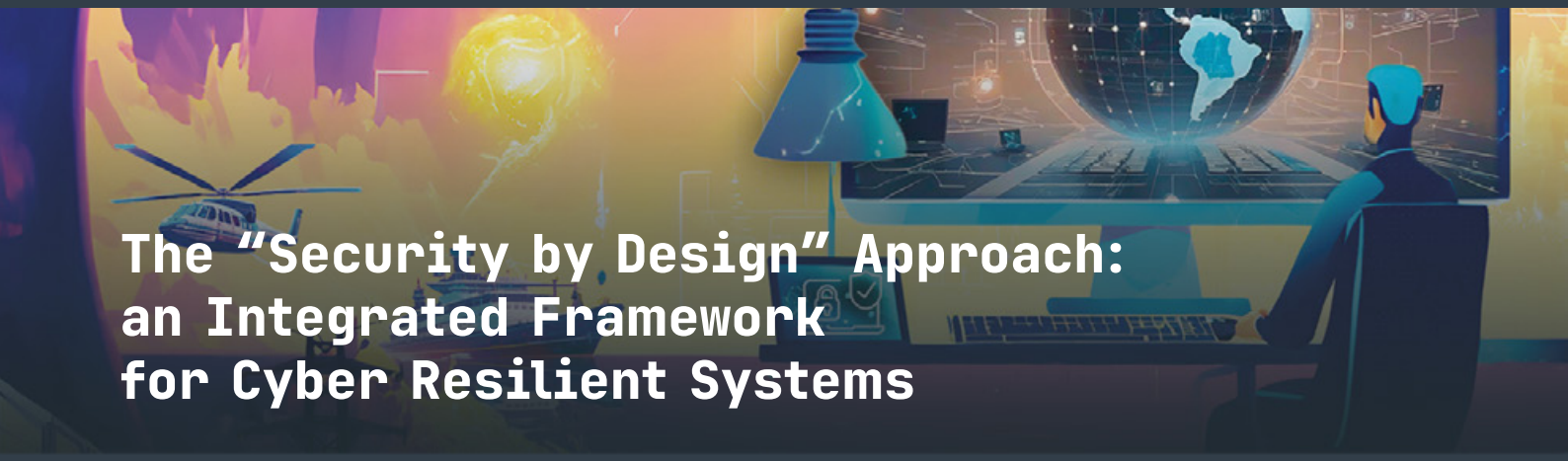
A shared taxonomy is the key factor that enables the cooperation of government and industrial entities to rely on safe and secure services even in presence of adverse conditions, in order to design, implement, and maintain cyber resilience of complex, hybrid, and multi-domain ecosystems.

Gabriele Cicognani: gabriele.cicognani@leonardo.com
Stefano Bordi: stefano.bordi@leonardo.com

Emanuele Angelitti: emanuele.angelitti@leonardo.com
Paolo Di Serio: paolo.diserio@leonardo.com
Alessio Caforio: alessiopiergiovanni.caforio@leonardo.com
Virginia Gugliotta: virginia.gugliotta@leonardo.com

REFERENCES

[1] https://insights.sei.cmu.edu/blog/system-resilience-what-exactly-is-it/, [Online].
[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454, [Online].
[3] https://www.ecb.europa.eu/paym/cyber-resilience/html/index.en.html, [Online].
[4] George Sharkov, "From Cybersecurity to collaborative Resiliency", SafeConfig '16: Proceedings of the 2016 ACM Workshop on Automated Decision Making for Active Cyber Defense, 26 October 2016.
[5] F. Björck, M. Henkel, J. Stirna and J. Zdravkovic, "Cyber Resilience–Fundamentals for a Definition," New Contributions in Information Systems and Technologies: Volume 1, vol. 1, pp. 311-316, 2015.
[6] https://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf, [Online].
[7] https://www.nist.gov
[8] https://www.mitre.org
[9] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1r1.pdf, [Online].
[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf, [Online].
[11] Leonardo Directive on "Cyber resilience in the life cycle of products and services", Rev. A, December 2022
[12] North Atlantic Council, "NATO Primary Directive on Information Management", 27 November 2008, C-M(2008)00113(INV), NATO Unclassified.



The "Security by Design" Approach: an Integrated Framework for Cyber Resilient Systems

Daniela Ferrarella, Fabio Varriale, Emanuele Angelitti, Stefano Bordi, Gabriele Cicognani

Leonardo – Cyber & Security Solutions Division

Nowadays, the "security by design" is an organization duty of care. A wide variety of actions can be taken to meet duty of care on security by design, from the onboarding of security specialized personnel to the adoption of security frameworks. The aim of this article is to provide a framework for a system development life cycle that integrates the cyber security and resiliency processes and constructs as issued by the National Institute of Standard and Technology (NIST) Special Publications (SP) 800-160 Volume 1 and Volume 2. This article also provides an application of the identified integrated framework to the space System Development Life Cycle based on the ECSS standard.

INTRODUCTION

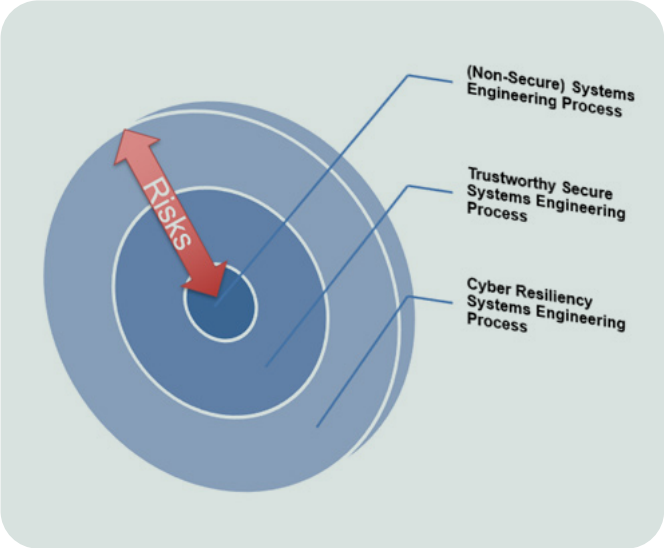
The development of "secure by design" (SbD) products (or systems) that meet the user requirements and the protection needs, calls for integrating cyber security and resiliency aspects derived from specific frameworks and standards into consolidated engineering system life cycle processes. The study of an integrated framework designed by the Cyber and Security Solutions division of Leonardo (IF4CR-Integrated Framework for Cyber Resilience) includes the use of ISO/IEC/IEE 15288 [1] standard for the development of systems, combined with the NIST SP 800-160 v1 [2] for trustworthy secure system, the NIST SP 800-160 v2 [3] for cyber resilient system and the NIST SP 800-37 [4] for security risk management.
The aim is to identify a common framework for the development and deployment of trustworthy secure and cyber resilient systems, which can be then tailored to the different system/product/service engineering life cycles of Leonardo. This article provides an example of the implementation of the integrated framework to space systems developed in accordance with the European Cooperation for Space Standardization (ECSS) standards.
The implementation of the IF4CR combined with the Leonardo Engineering Assurance Profile for Cyber Resilience analysis tool (LEAP4CR), enforces the leadership and commitment of the Cyber & Security Solutions Division of Leonardo, with respect to the secure-by-design paradigm.

OVERVIEW OF THE FRAMEWORK AND REFERENCE STANDARDS

This section provides an overview of the IF4CR, and the international standards implemented in this integrated framework that are:

- The ISO/IEC/IEEE 15288:2015, System and Software Engineering – System Life Cycle Processes [1];
- The NIST SP 800-160 v1r1, Engineering Trustworthy Secure System [2];
- The NIST SP 800-160 v2r1, Developing Cyber-resilient Systems [3];
- The NIST SP 800-37 r2, Risk Management Framework (RMF) for Information Systems and Organizations [4].

Finally, an overview of the ECSS-E-ST-10C-Rev1 standard for space system engineering is also provided, to support the case study.



1 – Structure of the integrated framework

THE INTEGRATED FRAMEWORK

The IF4CR transforms natively non-secure engineering processes into trustworthy secure and cyber resilient processes to use for the SbD. The IF4CR is an onion structure, in which each stage of the system development [1] is augmented by added-value layers that include risk-based [4] security [2] and cyber resiliency [3] activities (Figure 1).
The integrated framework trustworthy secure and cyber resiliency activities complete and support the delivery of the Organization's business objectives and manage security risks in line with the stated risk appetite. The SbD is not confined to the traditional information security, but it is conceived as the combination of risk-based information security, cyber security, and cyber resiliency decisions since the early stages of the ISO/IEC/IEEE 15288 [2] and throughout the entire life cycle of the system.

Table 1 provides the integrated framework based on the stages of ISO/IEC/IEEE 15288 in [1].
The IF4CR is intuitive because it is based on S.M.A.R.T (Specific, Measurable, Achievable, Relevant, Time-Bound) activities; it is standardized because based on proven and universally recognized standards. It is also adaptable because it is sufficient to map the steps of every existent engineering process to the six (6) stages of ISO/IEC/IEEE 15288 in [1], to have a complete SbD framework (see the case study).

ISO/IEC/IEE 15288:2015: "System and Software Engineering – System Life Cycle Processes"

Concept	Development	Production	Utilization	Support	Retirement

2 – Stages of ISO 15288

It is a world-wide international standard for systems and software engineering and system life cycle processes. It provides a set of four groups of processes that can be applied to a life cycle model representing the progression of the system itself through a series of six stages, from the initial concept to the final retirement. A representative system life cycle model is shown in Figure 2.

Table 1 provides the definition and description of the life cycle stages through which a system progresses on. The "*Stage*" is defined in the standard as "*a period within the life cycle of an entity that relates to the state of its description or realization*".
In the integrated framework only the fourteen technical processes of the standard are considered.

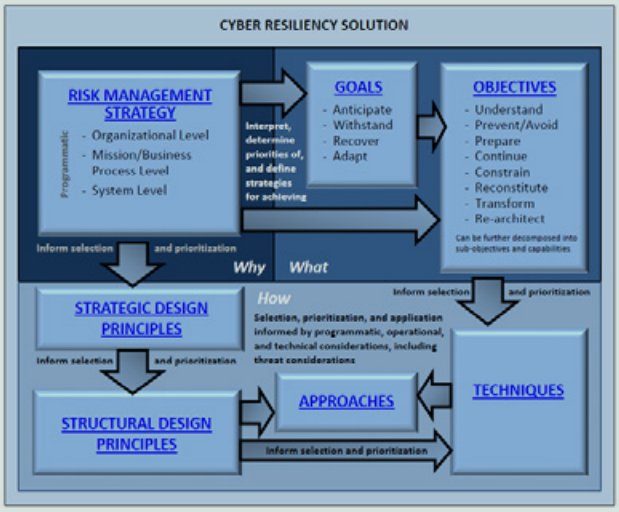
NIST SP 800-160 v1r1: "Engineering Trustworthy Secure Systems"

This document presents a systems security engineering framework within which the systems security engineering activities, aligned to the processes defined in [1], are performed. It gives a basis for establishing principles, concepts, activities, and tasks for engineering trustworthy secure systems.

In the standard context, security is defined as "*freedom from those conditions that can cause a loss of assets with unacceptable consequences*" and, therefore, security engineering is oriented to the protection of assets.

Integrated framework for the development and deployment of trustworthy secure and cyber resiliency Systems (IF4CR)			
ISO/IEC/IEEE 15288 stages	ISO/IEC/IEEE 15288 (macro) stage's purpose	NIST SP 800-160v1	NIST SP 800-160v2
Concept	- Identify mission requirements and stakeholder's needs - Explore concept of operations - Propose viable solution(s)	- Identify security mission requirements and security stakeholder's needs - Extend concept of operations to security use cases - Propose viable security solution(s) based on risk assessment	- Identify cyber resiliency mission requirements and cyber resiliency stakeholder's needs - Extend concept of operations to cyber resiliency security use cases - Propose viable cyber resiliency solution(s) based on risk assessment
Development	- Refine system Requirements - Create solution description - Built system - Verify and Validate System	- Refine system security Requirements - Create security solution description - Built system based on risk-based (RA "As -Designed") security principles - Verify and Validate system security solutions	- Refine system cyber resiliency Requirements - Create cyber resiliency solution description - Built system based on risk-based (RA "As -Designed") cyber resiliency principles - Verify and Validate System cyber resiliency solutions
Production	- Produce system - Inspect and test	- Produce risk-based security system (RA "As -Built") solutions - Security inspection and test	- Produce risk-based system (RA "As -Built") cyber resiliency system solutions - Cyber resiliency inspection and test
Utilization	- Operates system to satisfy users' needs	- Operates system in accordance with Security Operating procedures (SecOps) to satisfy users' needs	- Operates system in accordance with Cyber resiliency Operating procedures (CROps) to satisfy users' needs
Support	- Provide sustained system capability	- Provide sustained system security capability	- Provide sustained cyber resiliency security capability
Retirement	- Store, archive or dispose the system	- Store, archive or dispose the system in accordance with SecOps	- Store, archive or dispose the system in accordance with CROps

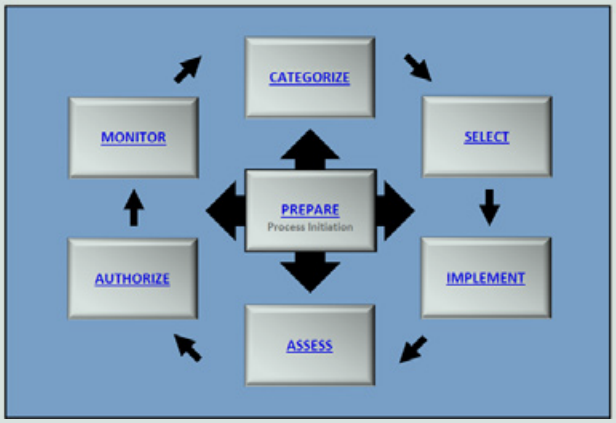
Table 1 — IF4CR vs ISO/IEC/IEEE 15288 stages and their purposes [5]



3 – Relationship among cyber resiliency constructs [2]

NIST SP 800-160 v2r1: "Developing Cyber-resilient Systems"

This publication focuses on "*cyber resiliency engineering and intends to architect, design, develop, implement, maintain, and sustain the trustworthiness of systems with the capability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises that use or are enabled by cyber resources*" [3].
The cyber resiliency concepts are represented by constructs that are the "building blocks" of the framework and consist of *goals, objectives, techniques, implementation approaches, and design principles (strategic and structural)*. A cyber-resilient system is the result of the engineering selection, prioritization, and application of the cyber resiliency design principles, techniques, and implementation approaches as described in Figure 3. There is a relationship among the constructs that can be interpreted in different ways, depending on stages of the system life cycle. In this publication the cyber resiliency engineering is intended as a specialty discipline of the systems security engineering.



4 – Risk Management Framework

NIST SP 800-37 r2: "Risk Management Framework (RMF) for Information Systems and Organizations"

This publication delivers guidelines for applying a Risk Management Framework to information systems and organizations, as well as provides a disciplined, structured, and flexible process for managing security and privacy risk.

It recommends the implementation of the RMF such as "*it is indistinguishable from the routine System Development Life Cycle (SDLC) processes carried out by organizations*" [4], thus aligning the RMF tasks with the activities running in these processes. The execution of the RMF tasks connects the essential risk management processes at system level to the risk management processes at organization level, including in this way an organization-wide view of the risk management. There are seven steps in the RMF as described in Figure 4.

A CASE STUDY: APPLICATION OF THE INTEGRATED FRAMEWORK FOR THE DEVELOPMENT OF SECURE AND CYBER RESILIENT SPACE SYSTEMS

Even if the ECSS standard is not part of the framework, a short introduction regarding ECSS-E-ST-10C-Rev1 standard for space system engineering is also provided, to support the understanding of the case study.This ECSS standard describes the main technical activities related to the different stages (called "phases") in the life cycle of a space system. Each phase contains process-defined activities to ensure that the final product satisfies the mission and stakeholders needs. These phases are in order with:

- Phase 0 - Mission analysis/needs identification.
- Phase A - Feasibility.
- Phase B - Preliminary Definition.
- Phase C - Detailed Definition.
- Phase D - Qualification and Production.
- Phase E - Utilization.
- Phase F - Disposal.

Each of the project phases above includes end milestones in the form of project review(s), whose outcome determines the readiness of the project, before moving to the next phase.
The rest of section provides an example of how the IF4CR can be tailored to the non-secure by design ECSS space systems engineering life cycle.

The objective of this case study is achieved in two steps:

- 1st step: each phase of the ECSS engineering life cycle is complemented with and completed by the cyber resiliency constructs of [3] and the technical processes of [2];
- 2nd step: the ECSS integrated phases are then mapped onto the ISO stages defined in [5].

Although both phases and stages are representative of the evolution of a system, a stage includes one or more ECSS phases. In particular:

- The Concept stage [5] includes phase 0 and phase A of the ECSS standards.
- The Development stage [5] includes the phase B and phase C of the ECSS standards.
- The Production stage [5] includes the end of phase C and phase D of the ECSS standards.
- The Utilization and Support stages [5] include phase E of the ECSS standards.
- The Retirement Stage [5] includes the phase F of the ECSS standards.

It is worth noting that the technical processes defined in [2] are recursively and iteratively applied across the whole life of a system for a progressive refinement. In this case study, some aspects related to security (e.g., supply chain risk assessment, configuration management, change management incident management and disaster recovery, documentation as input and output in each stage) are intentionally omitted for room reasons. The integrated activities for each stage of [5] are provided as follow:

Concept Stage

The Concept Stage is "*executed to assess new business opportunities or mission assignments and to develop preliminary system requirements and a feasible architecture and design solution*" [5]. In terms of integrated framework, the concept stage includes the 0 and A phases decision points and activities of the ECSS, as well as the activities of the NIST standards that are proper of the IF4CR.

ECSS PHASE 0: Mission Analysis/ Needs identification

The ECSS engineering process for Phase 0 is characterized by the following decision points and activities [6][7]:

- **Phase 0 decision point**: Mission Design Review (MDR).
- **Activities**: (i) To produce a broad spectrum of ideas and alternatives for possible missions from which new programs and projects can be selected; (ii) To develop possible mission/system concepts and preliminary operations scenarios (in the ConOps); (iii) To draw system-level technical requirements; (iv) To characterize the expected performance with respect to the physical and operational environment; (v) To support the definition of the Mission Requirements.

ECSS PHASE A: Feasibility

The ECSS engineering process for Phase A is characterized by the following decision points and activities [6][7]:

- **Phase A decision point**: Preliminary Requirements Review (PRR).
- **Activities**: (i) To assess the technical and programmatic feasibility of the possible systems and operations concepts; (ii) To propose system and operations concept(s) and technical solutions (including model philosophy and verification approach) to meet the identified needs and to be further elaborated during Phase B; (iii) To develop final mission concept, preliminary management, and technical plans, system-level preliminary technical requirements, identify critical technologies and propose pre-development activities; (iv) To develop more mature Concept of Operations (ConOps); (v) To finalize the expression of the needs.

NIST 800-160 v1 Framework

The technical processes of this NIST standard included in the concept stage are respectively with the Mission/Business Analysis followed by the Stakeholder Needs and Requirements Definition. During this stage, the understanding of the mission problems or opportunities that are proper of the ECSS phase 0 is analyzed from a security perspective. The results from such security risk analysis on cyber events affecting the objectives of the mission are taken into account to elicit trustworthy security requirements to integrate in the Mission Requirements and ConOps. Phase A of the ECSS is supported by this framework to identify the stakeholders involved in the space mission. The stakeholder's need is evaluated in terms of risks and protection needs that are transformed in stakeholder's security requirements and security operating concepts (OpsCon). Also, the outcomes of the security risk assessment support the ECSS phase A to analyse candidate solutions from the security trustworthiness point of view.

NIST 800-160 v2 Framework

The processes proper of the NIST 800-160 v1 during the concept stage are repeated within a wider and advanced persistent threat (APT) ecosystem [8]. During the ECSS phase 0 of the Concept stage, the risks from threats impairing the mission/business processes supporting the space mission objectives are evaluated, to understand the cyber resiliency measures to apply against a compromise, and how they can be achieved throughout a given mission/business process, applying realistic expectations for the resilience of information technology.

The space mission objectives aligned and supported by a risk management strategy at mission level establish the priorities of the cyber resiliency goals and objectives needs that are reflected in the mission requirements. In Phase A of the ECSS, candidate cyber resiliency solutions are proposed and analyzed with respect to the prioritized cyber resiliency goals and objectives. Also, the risk assessment on representative scenarios that include activities and attacks of APT actors, is the input for the cyber resiliency design strategic principles to be reflected as stakeholder's needs in the stakeholder requirements and operational concepts (OpsCon).

NIST SP 800-37 Framework

Tier 2 addresses risk from a mission/business process perspective, by designing, developing, and implementing mission/business processes that support the missions/business functions identified in phase 0 of the ECSS. Tier 2 begins with the identification and establishment of risk-aware mission/business processes to support the organizational missions and business functions. Implementing risk-aware mission/business processes requires a thorough understanding of the ecosystem [8]. This understanding is a prerequisite to building mission/business processes that are sufficiently resilient to withstand a wide variety of threats, including routine and sophisticated cyber-attacks, errors/accidents, and natural disasters. A key output from the Tier 2 definition of mission/business processes is the selected risk response strategy for these processes within the constraints defined in the risk management strategy. The risk response strategy [9] includes identification of trustworthy security and cyber resiliency protection needs and the allocation of those needs across components of the process. The risk response strategy is the input to trustworthy security and cyber resiliency mission and stakeholder requirements as long as ConOps and OpsCon.

Development Stage

The Development Stage "*is executed to develop a system-of-interest that meets stakeholder requirements and can be produced, tested, evaluated, operated, supported and retired*" [5]. In terms of integrated framework, the development stage includes the B and C phases decision points and activities of the ECSS as well as the activities of the NIST standards proper of the IF4CR.

ECSS PHASE B: Preliminary definition

The ECSS engineering process for Phase B is characterized by the following decision points and activities [6][7]:

- **Phase B decision points**: System Requirements Review (SRR) and Preliminary Design Review (PDR).
- **Activities**: (i) To finalize "trade-off "studies, confirm technical solution(s) for the system and operations concept(s) and their feasibility with respect to programmatic constraints; (ii) To establish an initial baseline for the system preliminary definition; (iii) To demonstrate that the solution meets the technical requirements according to the schedule, the target cost, and the customer requirements; (iv) To support the System Requirements Review (SRR) and the Preliminary Design Review (PDR) and ensuring implementation of the SRR and PDR actions; (v) To define the development approach and plan of engineering activities (Prepare the disposal plan and release the verification plan).

ECSS PHASE C: Detailed definition

The ECSS engineering process for Phase C is characterized by the following decision points and activities [6][7]:

- **Phase C decision point**: Critical Design Review (CDR).
- **Activities**: (i) To complete the detailed design definition of the system at all levels in the customer-supplier chain; (ii) To perform the production, development testing and pre-qualification of selected critical elements and components; (iii) To complete assembly, integration and test planning for the system and its constituent parts; (iv) To demonstrate the capability to meet the technical requirements of the system technical requirements specification.

NIST 800-160 v1 Framework

The System Requirements Definition, System Architecture Definition and Design Definition are the principal technical processes of this NIST standard included in the development stage. During this stage the stakeholder's protection needs (as expressed in the stakeholder requirements) are the base for definition of the system security requirements [10]. The security requirements are allocated to the system architectural elements and the security-relevant architectural characteristics are transformed into trustworthy secure design characteristics. In this way, all the security aspects are integrated into a consolidated design solution.

NIST 800-160 v2 Framework

During this stage, the cyber resiliency is included in the system requirements engineering process for space systems and is expressed in the context of the system architecture and design by means of risk-based structural cyber resiliency design principles, techniques, and approaches.

NIST SP 800-37 Framework

Tier 3 includes risk management activities integrated into the system development life cycle of the organizational information systems. During the development stage, the more detailed the system, the more specific and credible the threat information or assumptions about the threat and the more the potential design-related vulnerabilities in the space system can be mitigated during this phase, by choosing less susceptible alternatives.
Refine Trustworthy security and APT threat-modelling to elicit risk-based system requirements and design needs are within the aim of this framework at this stage (Risk Assessment "As-Designed"). Supply chain risk during the acquisition phase of the space system is also an area of concern. To address the supply chain risk during the development stage, organizations implement specific security controls as deemed necessary by the organization.

Production Stage

The Production Stage "*is executed to produce or manufacture the system-of-interest, to test it and to produce related enabling systems as needed*" [5]. In terms of integrated framework, the production stage includes the D phases decision points and activities of the ECSS as well as the activities of the NIST standards proper of the IF4CR.

ECSS phase D: Qualification and production

The ECSS engineering process for Phase D is characterized by the following decision points and activities [6][7]:

- **Phase D decision points**: Test Readiness Review (TRR), Qualification Review (QR), Acceptance Review (AR) and Operational Readiness Review (ORR).
- **Activities**: (i) To complete manufacturing, assembly, integration, verification and testing of flight hardware/software and associated ground support; (ii) To complete the interoperability testing between the space and ground segment (System Validation Test); (iii) To finalize the development of the system by qualification and acceptance; (iv) To finalize the preparation for operations and utilization.

NIST 800-160 v1 Framework

Implementation, Integration, Verification, Transition and Validation are the principal technical processes of this NIST standard included in the production stage.
At this stage, all the trustworthy security aspects of the

space system implementation are verified and validated to provide objective evidence that the system fulfils its specified security requirements and characteristics at every level, from system back to mission requirements. Successful verification and validation provide the readiness for the system to use in its intended operational environment, in a trustworthy secure manner. Vulnerability and Penetration testing (VAPT) are of a paramount importance at this stage.

NIST 800-160 v2 Framework

During this stage the cyber resiliency solution is implemented, and its effectiveness is evaluated. The verification and validation strategy for the cyber resiliency requirements includes adversarial testing or demonstration in a stressed environment with adversarial persistent activities. This means that it is necessary to validate the system's ability of achieving its mission objectives despite the attacks, and assuming that different system elements have been compromised. During the transition, threat and APT-informed training for all the operators necessary to the system utilization and support, is developed.

NIST SP 800-37 Framework

The production stage of the system development life cycle provides an opportunity for the organization to determine the effectiveness of the selected security controls employed within, or inherited by, the information systems under development, prior to the commencement of actual operations. Given the current threat information that is available to organizations, the organizational assumptions about the threat, the information discovered during effectiveness assessments, and the potential adverse impacts on organizational missions/business functions, it could be necessary to modify or change the planned implementation of the information system. Risk-related information can be developed to justify the proposed changes stage (Risk Assessment "As-Built").

Utilization & Support Stages

The Utilization Stage "*is executed to operate the product, to deliver services within intended environments and to help achieve continuing operational effectiveness*" [5], whereas the Support Stage "*is executed to provide logistics, maintenance, and support services that enable continuing system-of-interest operation and a sustainable service*" [5].
In terms of integrated framework, the utilization and support stages include the E phases decision points and activities of the ECSS as well as the activities of the NIST standards proper of the IF4CR.

ECSS phase E: Utilization

The ECSS engineering process for Phase E is characterized by the following decision points and activities [6][7]:

- **Phase E decision points**: Flight Readiness Review (FRR), Launch Readiness Review (LRR), Commissioning Results Review (CRR) and the End-of-Life review (EOL).
- **Activities**: (i)To support the launch campaign; (ii) To perform all activities at space and ground segment level to prepare the launch; (iii) To conduct all launch and early orbital operations; (iv) To perform on-orbit verification (including commissioning) activities; (v) To perform all on-orbit operations to achieve the mission objectives; (vi) To perform all ground segment activities to support the mission; (vii) To perform all other ground support activities to support the mission; (viii)To finalize the disposal plan.

NIST 800-160 v1 Framework

During these stages, the activities of this framework are mainly focused on verifying that the system is operated in a secure way and that the security aspects of products, services, and operator-system performance are monitored, as well as the security-relevant operational anomalies that are identified and analysed to securely sustain the capability of the space system to provide the services.

NIST 800-160 v2 Framework

The cyber resilience plays an important role at this stage. This framework highlights the need to operate the system to meet its mission assurance, business continuity, or other security requirements in an APT environment. Monitoring of the cyber resiliency solutions in the operational environment can be used to identify new or modified requirements, to revisit the constraints on techniques and approaches, to upgrade/modify capabilities, consistently with changes as noted [5]. It is worth noticing that the maintenance of the system or system elements can include the integration of new cyber resiliency solutions into the system [2]. The Incident response management and the disaster recovery are the other main aspects of cyber resiliency of the space system at this stage.

NIST SP 800-37 Framework

The monitoring of security control effectiveness and any changes to the system (e.g., patches) as well as the environments in which the space system operates, ensure that selected risk response measures are operating as intended on an ongoing basis.

Ongoing monitoring is paramount to maintaining situational awareness of risk to organizational missions and business functions that is critical to making the necessary course corrections when the risk exceeds the organizational risk tolerance.

Retirement Stage

The Retirement Stageit "*is executed to provide for the removal of a system-of-interest and related operational and support services, and to operate and support the retirement system itself*" [5].

In terms of integrated framework, the retirement stage includes the F phase decision point of the ECSS with the associated activities as well as tasks, activities and application of the concepts and constructs of NIST special publications.

ECSS phase F: Disposal

- The **Phase F decision point** is the Mission Close-out Review (MCR).
- The **activities** in this phase are described in [6] and in [7] and are presented in the following: (i) To implement the systems decommissioning/ disposal plan developed in Phase E.

NIST 800-160 v1 Framework

The main activities to perform in this framework are briefly presented to provide the aspects needed to securely end the existence of a space system element or system for a specified use, and securely preserve or destroy the associated data and information.

NIST 800-160 v2 Framework

The main activities in this framework consist of analyzing whether the removal of some system elements could decrease the cyber resilience and introduce potential vulnerabilities, as well as in evaluating the impact of the disposal process on the cyber resilience objectives of the systems, missions, and business functions in the operational environment, to define whether it was necessary to upgrade or modify the capabilities of other systems.

NIST SP 800-37 Framework

During the disposal phase of the system development life cycle, prior to disposal it is a standard procedure for organizations to verifiably remove any information from the information systems which if compromised may cause adverse impacts, and also to assess any risk associated with these activities.

CONCLUSIONS

The aim of this work is to define a version one (1) of a secure and cyber resilient System Development Life Cycle (SDLC) that integrates the security and cyber resiliency technical processes and constructs of the two frameworks developed by NIST in [2] and in [3] and the Risk Management framework in [4], within the system engineering activities defined by ISO/IEC [1]. A case study of the application of this version one (1) of the integrated framework to a Space System life cycle based on ECCS is also provided, to demonstrate the ease of use of this framework for all the products of Leonardo. A second version of this integrated cyber secure and resilient System Development Life Cycle is under development for further improvements.

Daniela M. Ferrarella: danielamaria.ferrarella@leonardo.com
Fabio Varriale: fabio.varriale@leonardo.com

REFERENCES

[1] International Standard ISO/IEC/IEE 15288, First edition 2015-05-15, Systems and software engineering-System life cycle processes
[2] NIST Special Publication NIST SP 800-160v1r1: Engineering Trustworthy Secure Systems, November 2022
[3] NIST Special Publication 800-160, Volume 2, Revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach
[4] NIST Special Publication 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy, December 2018
[5] International Standard ISO/IEC/IEE 24748-1, First edition 2018-11, Systems and software engineering-Life cycle management-Part 1: Guidelines for life cycle management
[6] ECSS-E-ST-10C Rev.1, System engineering general requirements, February 2017
[7] ECSS-M-ST-10C Rev.1, Project Planning and Implementation, March 2009
[8] INTERNATIONAL STANDARD ISO/IEC 27005, Information security, cybersecurity and privacy protection — Guidance on managing information security risks, Ott/2022
[9] NIST Special Publication 800-39, Managing Information Security Risk Organization, Mission, and Information System View, May/2011
[10] International Council on Systems Engineering (INCOSE), System Engineering Handbook v5, Systems Engineering Handbook (incose.org)

Leonardo Engineering Assurance Profile for Cyber Resilience

Mariano Pirrò, Enrico Giacobbe, Emanuele Angelitti, Stefano Bordi, Gabriele Cicognani

Leonardo – Cyber Security & Solutions Division

In an increasingly critical operating environment from the point of view of cybersecurity (also defined as the "cyber contested environment"), the cyber resilience of products used in increasingly complex solutions and platforms becomes the key point for dealing with both cyber and hybrid attacks. The Leonardo Cyber & Security Solutions Division therefore decided, in compliance to the Corporate Directive on the cyber resilience of internal products, to define a cyber resilience methodology (the LEAP4CR – Leonardo Engineering Assurance Profile for Cyber Resilience) that can be applied to both the existing products and projects as well as to those under development or of future design. Leonardo Cyber & Security Solutions Division is implementing adequate cyber resilience measures for all its own products in the portfolio, throughout their entire life cycle, and proposes itself as the point of reference on cyber resilience issues for the other Leonardo Divisions, due to the multi-domain characteristic of the proposed methodology.

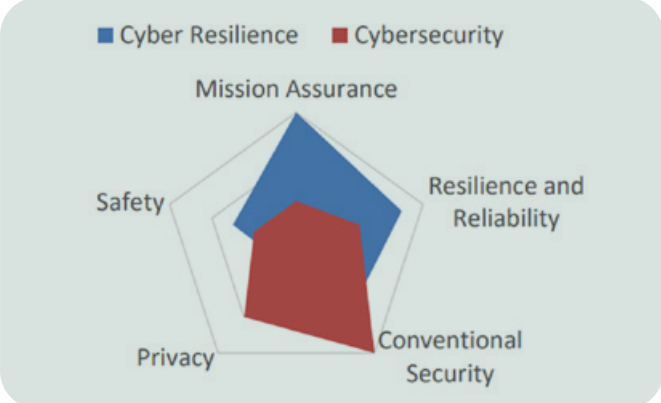
INTRODUCTION

In an increasingly digital and connected society and economy, the development of systems that relies on the functional-based approach only, is outdated. Security and trustworthiness of information are increasing their relevance every day. New opportunities and perspectives introduced by this scenario require a strategic and innovative approach that goes beyond the traditional Cyber Security. This is needed to ensure that systems can accomplish their duties and tasks (Mission Assurance) even in challenging cyber risky contexts, in order to safeguard sustainability of the business and reputation, as well as interests of the stakeholders.

The NIST Special Publication 800-160, Volume 2, Revision 1 [1], defines Cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources".

Cyber Resilience overlaps with, and builds upon, aspects of trustworthiness, in particular with resilience and conventional security. Similarly, Cyber Security encompasses conventional security in its care of prevention and protection, and overlaps with conventional reliability and resilience as it includes restoration as well.

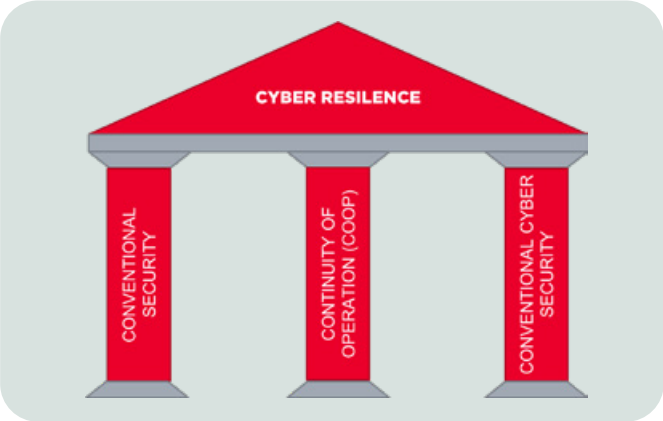
From this perspective, the notional relationships between cybersecurity and cyber resilience, and conventional security (with its focus on confidentiality, integrity, and availability of information), conventional resilience and reliability (with a focus on non-adversarial threats), safety, privacy, and mission assurance can be represented as in Figure 1.



1 – Conceptual relationship of Cybersecurity and Cyber Resilience with trustworthiness dimensions [2]

It is possible to say that Cyber Resilience builds on the following three pillars (Figure 2):

- **Conventional Security** focuses on achieving the security objectives of confidentiality, integrity, availability, and accountability (also known as Information Security) to acceptable levels, by using the combination of perimeter protections and internal controls [3];
- **Cyber Security** is the process of protecting digital information by preventing from, detecting, and responding to, attacks in the cyber space [4];
- **Continuity of Operations (COOP)** is a predetermined set of instructions or procedures that Figure 1 describe how mission-essential functions of an organization will be sustained within a determined period.



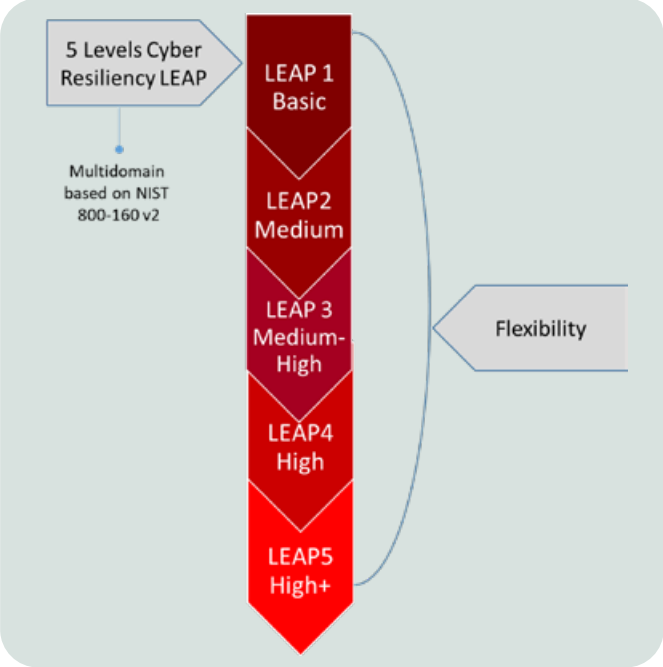
2 – Foundations of Cyber Resilience

C&SS DIVISION APPROACH TO CYBER RESILIENCE

In order to address the cyber resilience of its products and to comply with the Corporate Directive [5], the Leonardo Cyber & Security Solutions Division has launched the development of an Engineering Framework (the Leonardo Engineering Assurance Profile for Cyber Resilience – LEAP4CR) based on measurable and progressive levels (LEAPs). Such LEAPs are conceived for Leonardo's products first, but are potentially not limited to them. We repute this approach able to lead to strong strategic advantage, even in scenarios and marketplaces in which there are no as stringent contractual "cyber" constraints and requirements. It would also represent an opportunity for return on investment.

The higher the LEAP level, the higher and more complex are the security countermeasures in place (see Figure 3). This occurs both in terms of robustness of security mechanisms (more strength of the security measures) and in terms of assurance of application of security policies and security controls.

The LEAP4CR application framework outlines how to establish the Product LEAP target level and its actual set of applicable requirements. The LEAP levels feature the following main characteristics.



3 – Cyber Resilience LEAPs

- *LEAP1 – Basic.* Foundation: it focuses mainly on Cyber Security and Conventional Security by addressing Cyber Hygiene best practices (also with Cyber Security international standards or organizations practices such as ISO 27001, CIS, etc.). LEAP1 implements Cyber Resilience with a basic maturity level, because LEAP1 is typically designed for products that are not mission critical. LEAP1 is focused to maintain an acceptable security posture in order to guarantee Product functionalities. Every Leonardo Product should be associated to, at least, LEAP1.
- *LEAP2 – Medium.* Structured: this level guarantees a structured approach by introducing the Security Risk Analysis (SRA). The SRA is important to identify the risk exposure in terms of Cyber Resilience and to identify which safeguards must be introduced to reach an acceptable residual risk. The SRA activity has to be performed before delivery of the product in its operational environment. Safeguards specify technical, procedural and personnel requirements. LEAP2 also introduces more complex Cyber Resilience requirements in terms of architecture (mission awareness) and Security Operations Management.
- *LEAP3 – Medium-High.* Structured and mature: risk management activities add up to the SRA. As the SRA is iterated during product/system life cycle, the risk management is introduced with particular attention to Mission Assurance. This level typically represents target for Products featuring Medium level of Safety/Mission criticality.

- *LEAP4 – High*. Cyber Resilience-Centric: guarantees high coverage of Cyber Resilience techniques with strong positions on all its three pillars and on resilience specific techniques. Products categorised in this level have their own Cyber Resilience-centric focus and are Mission Orientated by implementing Automated Response techniques. Finally, the Cyber Security risk and mission assurance is managed and measured. Thus, the SRA is iterated, managed and applied with higher maturity. This level is the entry point for Products featuring High level of Safety/Mission criticality.
- *LEAP5 – High+*. Cyber Resilience optimised: guarantees the highest coverage of Cyber Resilience by introducing Cyber Resilience in a formal and structured way, since the early stages of development of the Product. The Cyber Security risk and mission assurance is managed, measured, optimised and pro-active. The SRA is iterated, managed and applied with the highest maturity.

In order to implement the characteristics described above, the methodology introduces five different areas of requirements coverage for each LEAP:

1. Mission Assessment & Control Definition;
2. Cyber Resilience Architecture;
3. Common Criteria Certification Target;
4. Secure Coding;
5. Security Operations Management.

The five areas listed above, according to the experience Leonardo Cyber Security Division, have been selected as necessary and sufficient to cover:

- The four pillars on which this framework is based (Figure 2);
- The Common Criteria Certification readiness (Common Criteria certification target);
- All the phases of the life-cycle of products (Analysis, Design, Implementation, Test and Operation).

ADVANTAGES OF LEAP4CR

The use of a structured framework such as LEAP4CR allows to obtain advantages in all the phases of a product's life cycle, through formalization and acceptance at all company levels. In particular, the process guarantees strong links with international standards, as per NIST 800-160 v2 rev.2, NIST 800-53 rev.5, MITRE Cyber Resiliency Design Principles. Security by design and throughout the whole products lifecycle is ensured through secure architecture, secure coding processes, security assessment, security testing, periodical risk analysis, and other security activities.

- Cyber Resilience Measurability is performed through the LEAP levels that can be used to address specific needs, in terms of cyber resilience, and to manage the evolution roadmap to achieve the needed level of LEAP.
- LEAP4CR provides links with certification schemes, that facilitate the needs of future certification activities through a direct mapping with security requirements and functions.
- The framework is also suitable to the Market positioning, as it is a sort of assurance of levels of the cyber resilience of Leonardo products that can give competitive advantages against market competitors. It can be used even as an accreditation to stakeholders and customers;
- LEAP4CR features Minor security maintenance costs overall the lifecycle: addressing cyber resilience in the early stage of design and development helps to keep investments low in remediation, in case of security incidents.

ADVANTAGES OF LEAP4CR

The LEAP4CR framework is valid for both products under development (referring to the security-by-design process) or for products already in operation (taking into account the improvement in security).
The presented methodology tailors the process described in the NIST SP 800-160 Vol 2 [1] and is composed by six steps. Such steps feature the following main characteristics that are also briefly descripted.

Understand the context. This activity consists of the analysis of the products under assessment. The analysis of the contexts (architectural, operating, mission, etc.) allows interpreting and prioritizing the Cyber Resilience needs, in order to define standards, regulations applicable to the contexts.

Establish the initial cyber resilience baseline. In this phase, a preliminary risk assessment is conducted, in order to gather information about the domain of the product, the type of data exchanged and how critical it is for the infrastructure. This helps in establishing the **Cyber Resilience LEAP target** for the products under assessment. The output of the context analysis provides the input for tailoring the requirements and the security controls frameworks in LEAP target. This step sets up the analysis of the initial capabilities, gaps and problems.

Analyse the system. Each part of the system is analysed in order to identify its components, their interactions and the data exchanged. This leads to understand "where the product is" in terms of identification of the current Cyber Resilience LEAP level. Depending on the product type, single components of the system could be considered as independent modules. Hence, there could be the need for having different LEAP targets for them, which are based on their criticality.

Define and analysis solutions. A gap analysis is conducted, in order to define the solutions/ integrations needed to upgrade the system from the current LEAP level to the target level. Then, all the discovered solutions are evaluated by taking into account the mission and the operational objectives, by using cost-effective & risk-based principles that will determine which ones will make it to the action plan for the implementation.

Develop the Action Plan. Depending on the single components identified in the previous phases and their target LEAP level, an integration priority is defined for each one of them that is based on the determined risk level and the integration impact on the system. The Action Plan shall also define the applicable approach related to the Common Criteria certification target, by specifying at system level or for sub-systems/ components when, where, and how to put in place functional and assurance requirements from this area. The selection of the best-fit solution will take into account a set of considerations such as the cost-effectiveness of implementing the requirements, the maturity level of the Products under assessment, etc.

Monitoring. The Action Plan is then applied iteratively and is continuously monitored with KPI calculations. In this way, even in case of existing Products, the LEAP target is reached incrementally (e.g. by addressing Cyber Resilience needs in the evolution of the Product). The KPI allows calculating the percentage of the LEAP target coverage. This measurement is very important especially in case of mature or operational products. Flexibility of the LEAP4CR framework emerges also in case of existing/mature products, as the re-engineering of the entire system could be very expensive and consequently not cost-effective.

4 – Steps for Cyber Resilience Analysis

However, a well-defined and monitored Action Plan allows reaching an acceptable threshold of LEAP coverage, also bringing concrete benefit for the products under assessment. At the same time, due to evolution/upgrade of the products, new developments will start by taking into account the requirements of the target LEAP. Following the iterative process target, as shown in Figure 4,LEAP could be incrementally reached in new releases of the product.

CONCLUSIONS

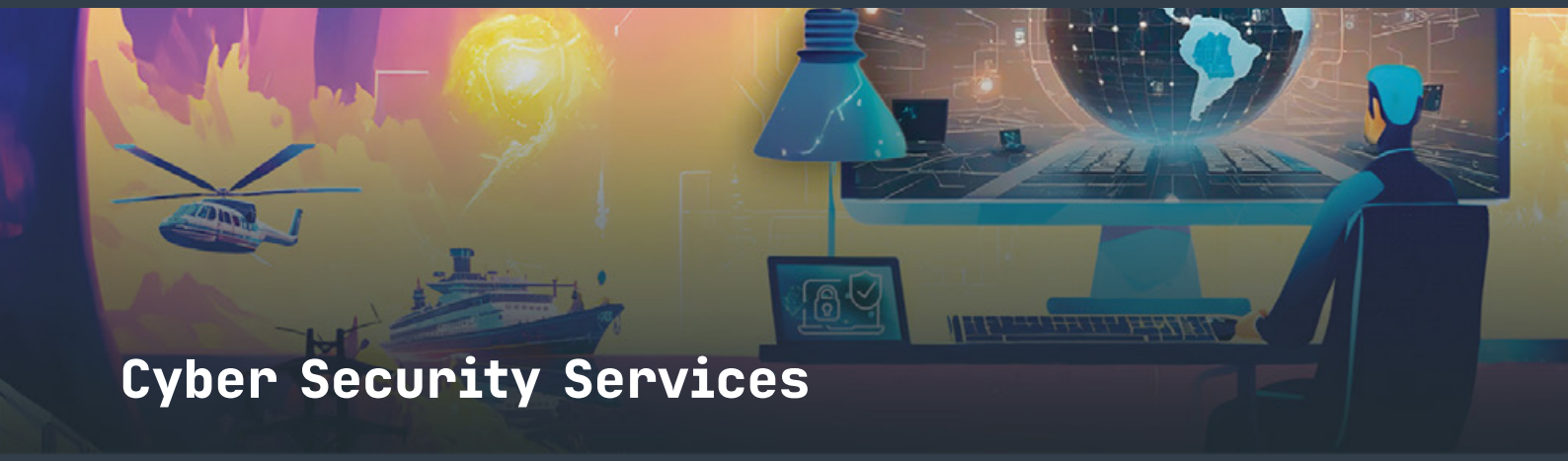
The concept and definition of the LEAP framework have interoperability and applicability in multi-domain contexts as its paradigms. Due to this capacity, LEAP is chosen as a corporate framework and candidates to support all Leonardo Divisions in products design, as an aid to the security by design and to the achievement and maintenance of adequate levels of cyber resilience over time.

Measurability of the cyber resilience guarantees monitoring the level of robustness of the systems over time, during all the lifecycle of products, from the earliest idea to their secure disposal, supporting all the engineering phases: design, development, operation, maintenance, evolution and disposal, guaranteeing rapid intervention in the event of cyber incidents and rapid restoration its standard operating conditions.

Mariano Pirrò: mariano.pirro@leonardo.com

REFERENCES

[1] R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, R. McQuaid, NIST Special Publication 800-160, Volume 2, Revision 1, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, December 2021
[2] Cyber Resiliency Design Principles, Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines, MTR170001 MITRE TECHNICAL REPORT, January 2017
[3] Cyber Resiliency Engineering Aid The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, May 2015
[4] Joint Task Force, Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 rev. 5
[5] UO CPOTO/Sviluppo Organizzativo, UO Security, UO CTIO/Chief Technology & Innovation Office, Cyber resilience nel ciclo di vita di prodotti e servizi, Revisione A, December 2022 - LDO – DI – 009 – A
[6] L. Zamburru, M. Malacario, R. Mosca, R.J. Graham, L. Giovannetti, M. Pirrò, P. Noli, N. Biundo, Leonardo Engineering Assurance Profile for Cyber Resilience (LEAP4CR) Framework, 25/11/2021.



Cyber Security Services

Enrico Giacobbe, Umberto Mosca, Aldo Sebastiani

Leonardo – Cyber & Security Solutions Division

The growing digitalisation of the society has given an unprecedented centrality to data and has turned it into an asset of inestimable value underlying the functioning of today's society. Cyber resilience of products, systems and systems-of-systems depends also on integrity, confidentiality, and availability of their data, field in which Cyber Security Services have a central role. At the same time, the massive use of Artificial Intelligence (AI) has opened new frontiers in cyber protection, but it has also triggered unique challenges related to complexity and speed of emerging threats. In this context, to face multi-dimensional threats it is crucial to adopt an approach based on reliable cyber security management, by leveraging on the synergy between the centrality of data, the deep knowledge of the cyber threats and the massive use of Emerging Disruptive Technologies. In a scenario in which threats are constantly evolving, this approach must drive the evolution of security services to mitigate cyber risks by improving data security and cyber resilience of products, systems, and systems-of-systems.

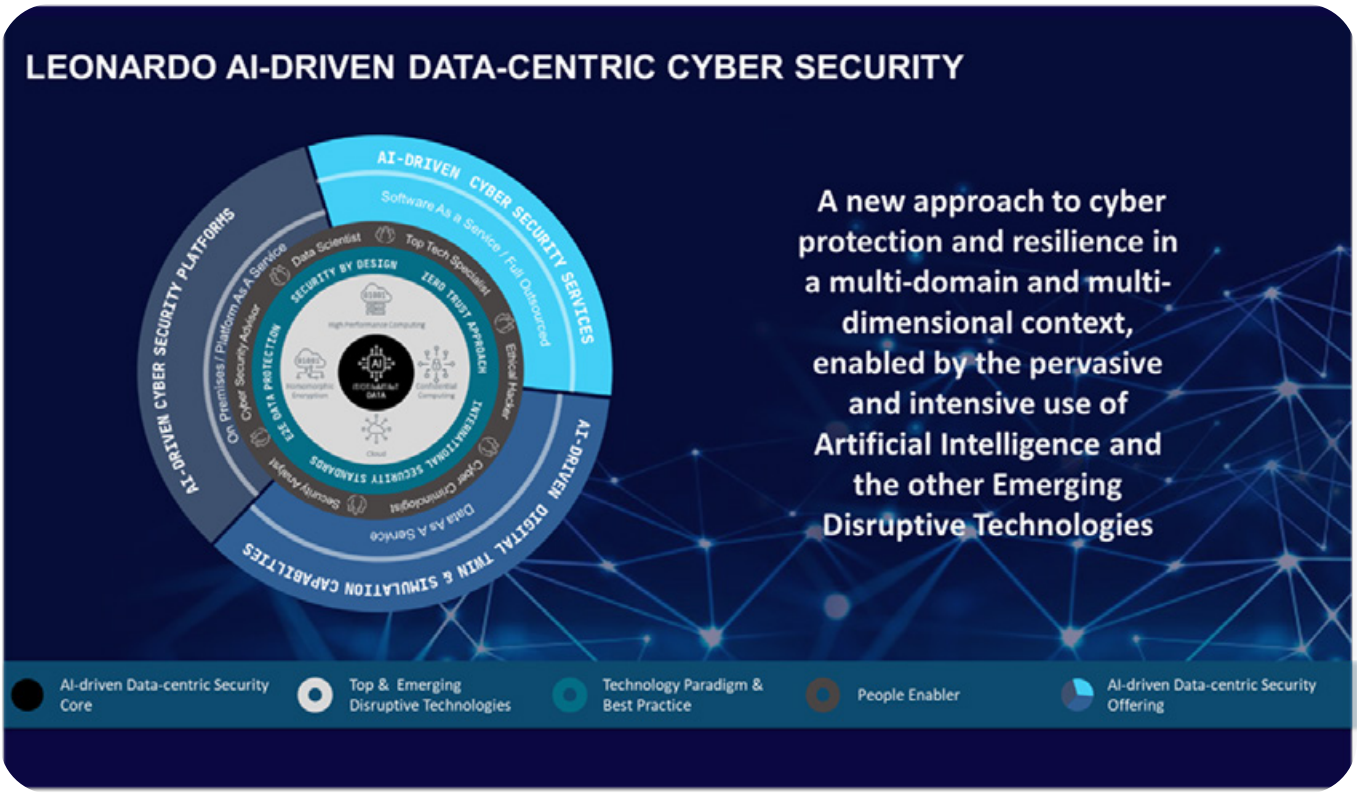
INTRODUCTION

In today's society, data has become an asset of inestimable value in our lives, as it influences the way we communicate, work, and make decisions. The increasing interconnection of our digital world underscores the paramount importance of safeguarding this resource. Cyber resilience of products, systems and systems-of-systems depends on integrity, confidentiality and availability of data, since these are fundamental aspects to maintain the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks or compromises on systems that use or are enabled by cyber resources [1]. As our reliance on data grows, the need for reliable cyber security measures becomes critical to protect against potential threats, as well as to ensure integrity, confidentiality, and availability of the information. This dynamic relationship between centrality of data and cyber security underscores the pivotal role that the latter plays in shaping security and functionality of our modern society.

Moreover, the landscape is dynamically transformed by Emerging Disruptive Technologies (EDT). These innovations not only offer new opportunities but also usher in a new era of cyber security challenges, as cybercriminals increasingly leverage on artificial intelligence to orchestrate more sophisticated and targeted attacks. The use of AI grants malicious actors the ability to automate tasks, adapt strategies in real-time, and exploit vulnerabilities with unprecedented efficiency. Thus, understanding and countering the evolving landscape of AI-driven cyber threats becomes increasingly important in fortifying digital defences. In this context, it is crucial to adopt a cyber security approach based on the synergy among centrality of the data, deep knowledge of the cyber threats and massive use of Emerging Disruptive Technologies, as the basis of innovative strategies.

The Data-Centric Security AI-Driven approach (Figure 1) is focused on data protection based on the widespread and pervasive use of emerging technologies, such as Artificial Intelligence enhanced by the use of High Performance Computers (HPC), that provides a fundamental contribution to the performance and scalability of the adopted computational models. These elements are enabling factors for the industrial scalability and enhancement of the Cyber Threat Knowledge Base that enables the provision of innovative

services oriented to Attack Prediction, evolves Detection & Response using Hyper Automation and allows creating new Cyber Recovery capabilities based on innovative paradigms.
The widespread and pervasive use of emerging technologies necessarily involves the evolution of the skills of security specialists, transforming the roles of security analysts into professional figures with strong skills in analysis, processing and data management with native use of Artificial Intelligence. It is essential to acquire multidisciplinary skills to understand, analyse and respond to threats increasingly characterized by multidimensional elements and to adopt the Zero Trust Approach in the current data-centric and interconnected context.



1-Data-Centric Security AI-Driven approach

CYBER DEFENCE AND NIST CYBER SECURITY FRAMEWORK

The National Institute of Standards and Technology (NIST) provides a Cyber Security Framework that represent a worldwide-recognized best practice for improving the security of data, products, systems, and systems-of-systems. Integrating cyber defence capabilities with the NIST Cyber Security Framework (CSF) [2] allows for a comprehensive and structured approach for a reliable cyber security management.
The framework shown in Figure 2 identifies six functions, whose objective is to address with a comprehensive approach all the cyber security life cycle within an organization. This means putting in place policies, procedures, technological assets and solutions, and operational capabilities that ensure cybersecurity is properly integrated into the organization's activities and aligned with business objectives, acting with a risk-based approach. CSF's functions are briefly described below:

2 – NIST Cyber Security Framework 2.0

- **Govern** – as cyber security relies on the risk management related to cyber threats, the Govern function is transversal, being it related to the establishing and monitoring of the risk management strategy and governance aspects.
- **Identify** – cyber defence starts from the accurate identification of the organization's digital assets, including critical systems, data, and resources, and from the evaluation of the risk they are exposed to. This function includes asset management, risk assessment and threat modelling, where data is the primary asset, and the Supply Chain Risk Management is also included.
- **Protect** – protection measures of digital assets, for instance technological security capabilities, access control, network segmentation, encryption, and regular security patching of systems, belong to this function and represent safeguards that prevent or reduce cybersecurity risk.
- **Detect** –real time detection of threats and anomalous activities is the scope of this function that involves the use of intrusion monitoring and detection systems to timely identify suspicious security activities.
- **Respond** –the ability to effectively and timely respond to security incidents is critical and is the scope of this function. Cyber defence must be ready to isolate threats, mitigate damage, and restore systems. An incident response plan should be put in place that clearly outlines the steps to follow in case of a security incident or a Cyber Crisis. This plan should include defined roles and responsibilities, communication strategies, and measures to put in place.
- **Recover** – After an incident, restoration of the affected systems and resumption of normal operations are essential. An organization must securely restore its services and operations as quickly as possible, while minimizing the impact on its business and essential services. This process includes restoring systems or data from backups, repairing system vulnerabilities, and implementing strategies to prevent from future cyberattacks.

The last two functions in this framework, Respond and Recover, are vital to address proper risk management and business continuity. The ability to provide effective rapid response to an incident and to restore systems and data, is critical to minimize the operational and reputational damage.

In fact, implementing a cyber security framework is not just about preventing from cyberattacks, as it is also about creating a resilient digital infrastructure that can withstand and recover from threats.

A cyber security framework is critical for data-centric organizations, especially to enable them to account for factors such as:

- **Protecting fundamental assets** - data and artificial intelligence models are invaluable assets for modern businesses. A comprehensive cyber defence integrated with all the functions of the Cyber Security Framework allows protecting these assets from cyber threats, also ensuring their confidentiality, integrity, and availability.
- **Legal and regulatory compliance** - with data protection laws becoming increasingly stringent around the world, a comprehensive cyber defence integrated with all the functions of the Cyber Security Framework allows ensuring compliance, also avoiding penalties and reputational damage.
- **Trust** - by demonstrating commitment and focus on cyber security, organizations can build trust with their customers, stakeholders, and partners.

Adopting cyber security services integrated through all the CSF functions provides a structured approach for reliable cybersecurity management, addressing the whole cyber security life cycle.

CYBER SECURITY SERVICES

The seamless evolution of cyber threats requires in-depth reflection on defence strategies and continuous development of new cyber security services. The ever-increasing complexity of threats requires not only constant adaptation of the existing defences, but also the adoption of innovative approaches to predict, detect, respond to breaches and recover from them. This innovation finds application on all the cyber security services, through the development of new capabilities and the improvement of effectiveness and efficiency of the already available ones, bringing improvements in the capabilities belonging to all the areas of the NIST Cyber Security Framework.

Identification & Protection

Prevention refers to the implementation of proactive security measures to protect data, products, systems, and systems-of-systems, moving towards threat prediction services. The landscape of cyber security services has undergone a remarkable evolution, driven by the imperative of enhancing prevention and prediction capabilities against cyber threats.

The integration of emerging disruptive technologies, such as Supercomputing and Artificial Intelligence (AI), play a pivotal role in fortifying cyber prevention and prediction capabilities.
Supercomputing has empowered prediction by allowing processing vast amounts of data swiftly enabling real-time threat analysis for prediction purposes, ushering in a new era of proactive defence, equipping organizations with actionable insights derived from comprehensive data collection and analysis.
Artificial intelligence, using algorithms specifically trained on Cyber Threat Knowledge Base and predictive analytics, stands as a cornerstone in the evolution of cyber security. By continuously learning and adapting to evolving threats, AI enhances the ability to forecast potential cyberattacks, thereby enabling pre-emptive measures. This enforces the shift from reactive to proactive defence strategies, marking a fundamental transformation in the cyber security paradigm.
The use of Supercomputing and Artificial Intelligence algorithms allows for the adoption of new methods of vulnerability analysis and the evolution of the Cyber Threat Intelligence as enabling elements for new types of services oriented to the prediction of potential cyberattacks.
The focus on predicting attacks, also exploiting dynamic situational awareness information, allows to evolve towards a proactive and customized protection.
By implementing product-specialized Cyber Threat Intelligence services, it is possible to dynamically analyse the technological vulnerabilities of a product, also in Operational Technology (OT) and embedded systems contexts, to constantly manage the vulnerability lifecycle and prevent possible impacting threats.
The emerging disruptive technologies have not only enhanced the efficacy of cyber security but have also introduced a dynamic and adaptive dimension to the threat mitigation. As the cyber landscape continues to evolve, the integration of Supercomputing and Artificial Intelligence in prevention services will remain instrumental in fostering a more resilient and anticipatory defence against the ever-evolving spectrum of cyber threats.

Detection & Response

Detection services include the implementation of processes and technological solutions to timely detect threats against products, systems and systems-of-systems. The use of advanced monitoring systems and behavioural analysis allows detecting suspicious activities or intrusions. Early detection is crucial to limit potential damages.
In the event of detection of a security incident, it is necessary to have available well-defined response procedures and to be ready to guarantee rapid response. Response services involve establishing incident response plans, performing rapid containment of the threat, executing Digital Forensics and Incident Response activities (DFIR), root cause analysis, managing communication internally and externally (including involvement of relevant authorities if necessary), and defining prioritized corrective measures.
In Operational Technology (OT) and embedded systems, adopting an on-board security agent on product and systems to probe internal networks and components allows to enable automated detection & response processes in multi-domain ecosystems, gaining visibility and threat response capabilities.
One of the emerging approaches in cyber detection and response is the Automated Detection and Response (ADR) that allows detecting and responding to security incidents, by leveraging Artificial Intelligence and Supercomputing to identify and mitigate potential threats in real time, with industrial scalability of threat detection and response capabilities, also by leveraging on Hyper Automation.
Key components of the ADR include:

- **Automatic threat detection**: it is performed through the use of artificial intelligence and behavioural analysis, to identify anomalous patterns or activities that may indicate a security threat;
- **Hyper automation in incident response**: the response to security incidents is automated through actions such as isolating affected systems, blocking malicious activities or triggering alerts for further investigations;
- **Continuous orchestration**: coordination of various security tools and processes to streamline incident response workflows;
- **Data correlation**: aggregation and correlation of data from multiple sources to provide a comprehensive view of potential security incidents;
- **Integration of advanced Cyber Threat Intelligence**: native use of advanced cyber threat intelligence to improve detection capabilities of potential cybersecurity risks.

The implementation of the ADR significantly improves the efficiency and effectiveness of a cybersecurity system thanks to shorter response times and reduces the impact of the incidents themselves.
Another emerging approach in the field of response to cyber incidents is the ability to adopt **Cyber Rapid Response Teams (CRRT)** in “field”. In practical terms, those teams should have tools capable of supporting high operational flexibility to intervene quickly and to apply the countermeasures that are necessary to react to threats in shorter as possible time.
The CRRTs are used as mobile teams to manage security incidents, intervening in critical security incident context on unknown infrastructures which can adopt heterogeneous technologies in the IT field

as well as in the OT (Operational Technology) and embedded systems fields.
To support and enable a truly effective intervention, those teams must have specific capabilities that guarantee the ability to operate on the infrastructures subject to the attack. This is obtained thanks to specific sensors, situational awareness capability for immediate understanding of the context of the specific incident, and an operational model that guarantees rapid flow of the information from the technical to the decision-making level and vice versa.
The Rapid Response Toolkit (RRT) framework supports the effective incident response with a strategic approach. In particular, it focuses on creating easily deployable, modular and scalable rapid response tools, to comprehensively support the response phase to major incidents. The Rapid Response Toolkit is a secure-by-design tool whose architecture and modules provide advanced functionality to support incident response and crisis management services. This solution is therefore able to support the management of IT incidents (detect, investigate, and remedy hostile activities) in different scenarios including the geographically distributed ones, with particular reference to government environments and critical information infrastructures, in the IT/OT/IoT contexts.

Recover

After an incident, restoring products, systems and systems-of-systems to normal operation and addressing the improvement actions are critical factors. Recover services include, as examples, Data Recovery (cleaning contaminated data or reconstructing lost data), Residual Impact Assessment, Continuous Improvement Planning, Disaster Recovery and Business Continuity.
With reference to new approaches in the recover field, in a context in which the digital infrastructures underlying strategic services are fully interconnected, it is increasingly important to adopt services and solutions that prevent or limit the propagation of significant cyberattacks, such as ransomware-type attacks.
The use of Backup and Disaster Recovery strategies does not always guarantee protection from ransomware-type attacks: attackers often try to delete or make the backup copies unusable before they make their presence evident by proceeding with data encryption and the ransom demand.
The Crisis & Recovery Vault (CRV) aims to complement the traditional processes, as it aims to prevent or limit the impact of cyber attacks by creating an isolated, immutable and independent vault environment. Inside it, the essential services and data (e.g. services underlying core system functionalities, especially in modern product, systems and system-of-systems) are protected, and the main services are directly provided from it, if necessary. Its objective is to guarantee the availability of core services and data by creating a technological infrastructure with logical and physical resilience characteristics that ensure the availability of essential services in the event of an extreme crisis. This solution uses innovative data protection technologies, such as the Confidential Computing, to provide end-to-end data protection encrypting the data in all its states (in transit, at rest, in use). This solution also includes the use of specific appliances to enable and disable data writing, the use of an air-gapped transmission mode and the use of a tool for Cyber Sanitization of data that is based on Artificial Intelligence algorithms trained on the Cyber Threat Knowledge Base, which allows data analysis and data reputation operations. The use of a sandbox environment permits safe recovery of data and applications, and allows the restoration of the minimum services required in coherence with each phase of the crisis management cycle, from the Readiness phase to the Responsiveness, up to the Recoverability phase.

PHYSICAL-LOGICAL SECURITY CONVERGENCE

The physical-logical security convergence is a strategic approach that recognizes the multi-dimensional interconnection of physical security and cybersecurity. It also aims integrating these two disciplines, to improve the organization's ability to address complex threats and security challenges [3]. Without a strategy that would drive the convergence of the logical and physical security worlds, their relevant risks could not be managed and efforts to pay should be duplicated. The physical-logical convergence recognizes that security threats maybe characterized from multi-dimensional shape and promotes the integrated approach, to more effectively mitigate those threats.

By integrating their physical and cyber security practices, organizations can increase their resilience and improve their ability to respond to complex and evolving threats. Such a convergence promotes the cooperation between the cyber security and physical security teams within an organization, which ensures more comprehensive protection. For example, the physical access to a data center can be restricted through biometric controls and electronic keys, while simultaneously the logical security protects data within that data center. This integration improves the overall resilience and threat response capability, by ensuring that the physical and digital aspects of security operate

in synergy to protect the organization from a wide range of risks. This is obtained through:

- **Monitoring and information sharing** - Information collected by physical security systems, such as surveillance cameras and motion detectors, can be integrated with data collected by information security systems, such as the network logs. Sharing this information enables faster detection and response to threats that involve both these aspects of security.
- **Coordinated Incident Response** - In case of incident or breach, a coordinated response is of critical relevance. The physical-logical convergence facilitates an integrated response in which the physical security and the cyber security personnel work together to identify, contain, and mitigate the incident.
- **Identity and Access Management (IAM)** - The physical-logical convergence can extend to the identity and access management, with the use of integrated IAM solutions that govern the access to physical and digital resources. This reduces the risks associated with compromised credentials or unauthorized access.
- **Advanced Detection Systems** - The convergence enables to use advanced detection systems, such as the anomalous behavioural detection, which can identify suspicious behaviour patterns in both information systems and physical access.
- **Training and awareness** - The security awareness among personnel is crucial as well. The physical-logical convergence can facilitate the training that covers both physical and cyber security aspects.
- **Scalability and Adaptability** - It is important to ensure that the integrated security strategy is scalable and adaptable to changing security threats and technological advancements.
- **Data Protection** – The integration of data protection measures, including encryption and data loss prevention, into the overall security strategy is a key aspect to safeguard sensitive information in both physical and digital forms.
- **Collaboration and Communication** - Consists of promoting collaboration and communication among the physical security and cyber security teams, to encourage the sharing of information and best practices and a cohesive approach to security.

The physical-logical convergence approach is essential to addressing the complexity of modern security threats. Cyber security services benefit from this integration, which enables more robust and coordinated defence against an ever-changing threat landscape.

CONCLUSIONS

In conclusion, ensuring comprehensive and structured approach for a reliable cyber security built upon worldwide recognized best practice and leveraging on emerging disruptive technologies is crucial to defend today's data-driven society and to guarantee resilience of products, systems, and systems-of-systems against evolving threats. By leveraging on disruptive cutting-edge technologies, organizations can navigate the dynamic landscape of cyber threats with greater confidence, by ensuring the integrity, confidentiality and availability of sensitive data that underpin essential services for Institutions, National Critical Infrastructures, Companies and Citizens.

Enrico Giacobbe: enrico.giacobbe@leonardo.com
Umberto Mosca: umberto.mosca@leonardo.com
Aldo Sebastiani: aldo.sebastiani@leonardo.com

REFERENCES

[1] https://csrc.nist.gov/glossary/term/cyber_resiliency
[2] https://www.nist.gov/cyberframework/framework
[3] Internal documentation of the Cyber & Security Division - Cyber Security & Digital Center

Challenges and Deal in Cyber Resilience, and Related Products

Fabio D'Ambrosi

Leonardo - Cyber & Security Solutions Division

In the relentless digital age, every facet of our lives is intricately interwoven with technology. Thus, the term "cyber resilience" has transcended its mere buzzword status, to become the bedrock of contemporary cybersecurity. Cyber resilience encompasses a multifaceted approach that extends beyond traditional security paradigms, and we need to acknowledge that threat. The intricate realm of cyber resilience dissects a range of sophisticated technological products meticulously designed to fortify our defences against cyber adversaries. These products form the vanguard of a relentless battlefront in which algorithms, data analytics, and cutting-edge technologies collide with the ever-evolving tactics of threats. In this paper, we go through details of such resilient guardians, by exploring their inner workings and capabilities, as well as the complexity of integrating them into a cohesive cybersecurity strategy.

UNDERSTANDING CYBER RESILIENCE

In the digital dominion, adversaries relentlessly probe for vulnerabilities and exploit them. Thus, the concept of cyber resilience arises as a fortress of adaptive security. It's not just about building walls: it's about creating an environment that can withstand, recover from attacks, and learn from them. To grasp the essence of cyber resilience, let's delve into its technical intricacies.

1 - Cyber Resilience definition

Defining Cyber Resilience

Cyber resilience transcends conventional cybersecurity, as it moves beyond the sole focus on prevention. It encompasses a proactive stance that anticipates and prepares for potential disruptions, emphasizing three core principles (see Figure 1):

- **Redundancy and Diversity** - Cyber-resilient systems intentionally diversify components and data storage to ensure seamless operation even when some of its elements go failing.
- **Rapid Detection and Response** - The ability to detect quickly threats and to react decisively, is fundamental to cyber resilience. This entails leveraging technologies like machine learning-based anomaly detection and automated incident response systems to minimize the dwell time, which is the period attackers spend within a network while being undetected.
- **Continuous Learning and Adaptation** - Cyber resilience involves learning from past incidents, to enhance future defenses. Security teams employ technologies such as threat intelligence platforms, to anticipate those emerging threats that are based on historical patterns and trends.

The Threat Landscape

Cyber resilience is the response to an increasingly complex and relentless threat landscape. Modern adversaries deploy advanced tactics, such as zero-day exploits and sophisticated malware, to infiltrate networks, pilfer data, and disrupt operations. Let's consider the example of a zero-day vulnerability – an unpatched software flaw unknown to the vendor. A cyber-resilient organization should have put in place processes enabling to swiftly respond, such as a robust zero-day attack response plan. The plan should include continuous threat intelligence gathering, prioritized vulnerability assessments, advanced detection mechanisms, rapid response team activation, isolation and quarantine procedures, patch management strategies, post-incident analysis, and continuous adaptation. This ensures organizations to be able to swiftly counter emerging threats and to maintain cyber resilience.

Importance of Cyber Resilience

To underscore the importance of cyber resilience, let's examine a real-world case: the 2020 SolarWinds supply chain attack. An unknown threat actor compromised SolarWinds' software updates, by infiltrating numerous high-profile worldwide organizations. The incident showcased the value of cyber resilience in action. Affected organizations with robust resilience mechanisms minimized that damage by swiftly identifying and mitigating the breach. This event highlighted that even the most sophisticated adversaries can be thwarted, when cyber resilience is the cornerstone of an organization's cybersecurity strategy. Understanding these technical intricacies is pivotal as we delve into the products designed to fortify cyber resilience, which are introduced by the subsequent sections of this article.

PRODUCTS FOR CYBER RESILIENCE

In our quest to bolster cyber resilience, it's crucial to acknowledge the pivotal role of:

- the cyber resilience governance approach;
- the products portfolio enhancement;
- the security by design life cycle.

As we have focused on the need for deployment and maintenance of cyber resilience products, let's now dissect how these concepts intertwine with the products designed to defend against digital adversaries.

The Cyber Resilience Governance Approach

A nice to have methodology serves as the nexus for overseeing and orchestrating cyber resilience efforts. The cross-functional integrated approach ensures collaboration across departments, by aligning business objectives with cyber resilience strategies. This ensures that governance is not siloed but permeates throughout the organization.

This method adheres to evolving standards, such as the NIST CSF (National Institute of Standards and Technology Cybersecurity Framework) v2 to ensure that the principles outlined in that standard are seamlessly integrated into its governance structure. This involves aligning the core functions of the framework with the organization's overall cybersecurity strategy. For example, the "Identify" function assists in understanding and managing cybersecurity risks, while the "Protect" function guides the implementation of safeguards that ensure the security of assets and data. Given the dynamic nature of cybersecurity threats, the methodology based on cyber resilience governance recognizes the importance of staying abreast of the latest developments in standards such as the NIST CSFs. Regular updates to the framework are monitored and compliance reviews are conducted, to assess the organization's adherence to the latest version of that standard.

By aligning with NIST CSF v2, this method demonstrates its commitment to adhering to the internationally recognized cybersecurity best practices. Such a commitment not only enhances the organization's ability to withstand cyber threats but it also fosters trust among stakeholders, partners, and regulatory bodies.

A diverse portfolio of cyber resilience products is crucial for addressing multifaceted threats. The following products play a pivotal role in fortifying the organization's defences:

- **Advanced MSS (supplied by Next Gen. OT-IT SOC) & CSIRT (federated)** - In the context of platform embedded cyber resilience, the Advanced Managed Security Services (MSS) offered by the Next Gen. OT-IT SOC assumes a pivotal role. By integrating proactive threat detection, incident response capabilities, and continuous monitoring functionalities, the Advanced MSS positions itself at the forefront of the new cyber resilience vision. Through the deployment of cutting-edge technologies, it provides real-time visibility into the dynamic threat landscape, allowing for swift identification and response to potential cyber threats. Moreover, the Advanced MSS's proactive stance aligns seamlessly with the ethos of platform embedded cyber resilience.

It strengthens the resilience of the ecosystem from within, by preemptively identifying and mitigating threats before they turn into full-blown incidents. This proactive approach not only minimizes the likelihood of cyber disruptions but also it bolsters the platform's capacity to adapt and evolve in the face of emerging threats. Furthermore, the federated Cyber Security Incident Response Team (CSIRT) model complements the Advanced MSS by fostering collaboration and information sharing across organizational boundaries. This collaborative framework enhances the platform's resilience by facilitating a coordinated response to cyber incidents. By leveraging collective intelligence and pooling resources, the federated CSIRT model reinforces the platform's ability to detect, respond to, and recover from cyber attacks in an efficient way. In essence, the Advanced MSS supplied by Next Gen. OT-IT SOC embodies the core tenets of platform embedded cyber resilience. By proactively detecting threats, facilitating rapid response, and promoting cross-organizational collaboration, the Advanced MSS plays a pivotal role in fortifying the resilience of the ecosystem and in safeguarding its integrity in the face of evolving cyber threats.

- **Cyber Situational Awareness** - This product provides real-time intelligence on the cyber threats landscape. By aggregating and analyzing data from various sources, it empowers organizations to anticipate and respond to potential threats, before they escalate.
- **Cyber Range** – It is a simulated environment for cyber exercises and training that allows organizations to test and enhance their cyber defense capabilities in a controlled setting. It facilitates the development of effective incident response strategies and the training of cybersecurity professionals.
- **Cyber Test Range** - This product allows organizations to evaluate the resilience of their systems and applications through controlled testing. By identifying vulnerabilities and weaknesses, organizations can proactively strengthen their cyber defenses.
- **Cyber Training** - The Cyber and Security Academy offers continuous education and skill development for cybersecurity professionals. It provides structured curriculum, hands-on training, and certification programs to ensure that the workforce is well-equipped to handle evolving cyber threats.

The Products Portfolio Enhancement

In the dynamic landscape of cyber threats, enhancing the organization's product portfolio is paramount for comprehensive cyber resilience. This section underscores the importance of adapting to challenges posed by the device diversity and by the remote workforce.

Given the proliferation of diverse devices and the widespread adoption of remote work, the attack surface has expanded exponentially. The Products Portfolio Enhancement strategy recognizes the need to address the device diversity, by encompassing various endpoints and networked devices. It acknowledges that a one-size-fits-all approach is insufficient in safeguarding against the myriad of threats posed by different devices and remote work scenarios.

Integrating security into the DevOps lifecycle known as DevSecOps, is instrumental in maintaining a proactive cybersecurity stance.

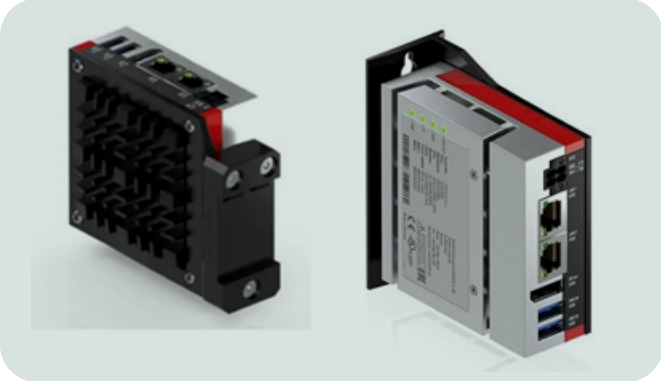
The Products Portfolio Enhancement approach involves the enhancement of DevSecOps practices to ensure that security is not a bottleneck but is an integral part of the development process. This includes automating security checks, integrating security tools into the development pipeline, and fostering a culture of collaboration between development, security, and operations teams. Recognizing the transformative power of Artificial Intelligence (AI), the Products Portfolio Enhancement strategy leverages AI in secure engineering practices. AI algorithms are employed to analyse and identify patterns that are indicative of cyber threats, to provide a proactive defence against evolving attack vectors. The Secure Engineering with AI ensures a dynamic and adaptive security posture that is capable of responding to - and learning from - emerging threats, in real-time.

In the context of cyber resilience, rigorous testing is mandatory. Test Automation is a key element of the Products Portfolio Enhancement strategy, streamlining the testing process for applications, systems, and networks. Automated testing tools enable rapid and repetitive testing, to ensure that vulnerabilities are identified and remediated efficiently. This approach is particularly crucial in the face of the device diversity, in which a multitude of platforms and configurations must be considered. As organizations increasingly integrate digital technologies into physical systems, securing the Cyber Physical Applications becomes paramount. The Products Portfolio Enhancement strategy includes specialized solutions designed to secure the convergence of digital and physical elements. This involves implementing robust access controls, encryption, and monitoring mechanisms, to safeguard the cyber-physical infrastructure from potential threats.

In conclusion, the Products Portfolio Enhancement strategy is not only about diversifying the toolkit but also about tailoring solutions to the evolving challenges posed by the device diversity and by the remote workforce. By embracing this approach, organizations can fortify their defence posture and

and ensure resilience against a wide spectrum of cyber threats.
In the dynamic landscape of cyber threats, the Products Portfolio Enhancement strategy aligns seamlessly with the LEAP4CR (Leading Practices for Cyber Resilience) standard, focusing on core tools that support and enhance cyber resilience. The LEAP4CR provides a comprehensive framework that integrates seamlessly into the organization's cyber resilience strategy.
This framework encompasses tools such as the Leonardo End Point Security (LENS), the Cyber Threat Intelligence System (CTIS), the Cyber Training, the Cyber Test Range, the Vulnerability Assessment and Penetration Testing (VA&PT). Let's go through its components:

- **DevSecOps Tool** - It is an advanced analyzer that focuses on both the process and the source code. It offers detailed analysis, executive summary, and custom reports for each finding, ensuring a comprehensive understanding of vulnerabilities and areas for improvement. The DevSecOps plays a pivotal role in the continuous improvement cycle, allowing organizations to iteratively enhance their security posture.
- **CTIS** - the integration of specialized threat intelligence to enhance proactive defense mechanisms, as the LEAP4CR emphasizes, includes leveraging threat feeds, indicators of compromise, and advanced analytics to anticipate and thwart potential cyber threats. The incorporation of the specialized threat intelligence provided by the CTIS within the LEAP4CR standard ensures that the organization remains well-informed about the evolving threat landscape.
- **LENS** – Leonardo End Point Security - the Endpoint security is a critical component of cyber resilience, as it offers real-time monitoring and response capabilities. The LENS enhances the organization's ability to detect and mitigate threats at endpoint level. It provides deep visibility into endpoint activities, supports the identification of malicious behaviours and facilitates a swift and targeted response. In this perspective, the LENS embedded solution could be applied on multidomain ecosystem (air, land, sea and space). An example of this approach is LENS-AIR (see Figure 2) for avionic\space systems that is the result of a design and subsequent development based on the paradigms described above but that can be operated to other domains as well. Specifically, the design and development of an End Point Security based on microkernel technology for embedded environments, multi-platform, and with functional compatibility with both traditional operating systems (Linux) and specific real-time systems, required a technologically advanced approach in both the design and implementation phases. The design applied principles for the minimization of privileges to ensure that each component of the system has only the strictly necessary permissions to perform its functions. The implementation, on the other hand, required the incorporation of anomaly detection mechanisms, along with robust error management, aimed at ensuring that the agent can continue to operate reliably even in adverse conditions.



2 – LENS-AIR probe version

- **Cyber Training** - Continuous education is vital in the realm of cyber resilience. The Cyber Security Academy, as part of LEAP4CR, provides structured training programs to empower cybersecurity professionals. It ensures that the workforce is updated to the latest knowledge level and skills, to effectively navigate and counteract emerging cyber threats.
- **Cyber Test Range** - The Cyber Test Range within the LEAP4CR toolkit is a dedicated environment for cyber exercising, testing, and training. It allows organizations to simulate real-world cyber scenarios in a controlled setting. The Cyber Test Range facilitates the evaluation of cyber defense capabilities and response strategies, as well as the resilience of systems and applications. It plays a crucial role in ensuring that the organization's cyber resilience is tested and validated under various conditions, to prepare cybersecurity teams to respond effectively to diverse cyber threats.
- **VA & PT** - The Vulnerability Assessment and Penetration Testing are integral elements of the LEAP4CR standard, which facilitate the identification and remediation of vulnerabilities before they can be exploited. This proactive approach strengthens the organization's overall cyber resilience posture by addressing potential weaknesses in systems, applications, and networks.
- **Security by design lifecycle Suite** - In fostering a proactive and resilient cybersecurity posture, the correct approach must include the implementation of a Security by Design Life Cycle Suite, which were meticulously designed to validate the cyber resilience

of products at every operation phase. Such a suite must employ a formal method that incorporates a series of "gates," to ensure that each stage of the product development undergoes rigorous scrutiny for cybersecurity considerations.

The integration of the LEAP4CR methodology and tools into the suite enhances its efficacy by providing a holistic and standardized approach to cyber resilience. The Security by Design Life Cycle Suite aligns with LEAP4CR's core principles, ensuring that cyber resilience is not an afterthought but it is an integral part of the development process. This formalized approach not only identifies potential risks early in the development process but it also establishes a culture of security consciousness throughout the organization. Furthermore, this methodology incorporates continuous monitoring of key cyber resilience indicators, which is a fundamental aspect of LEAP4CR's philosophy. Such a real-time monitoring ensures that any deviations from the established cyber resilience benchmarks are promptly detected and addressed. The integration of the AI support enhances the suite's capabilities, by providing intelligent insights and automating responses to emerging threats.

3 - Security by design lifecycle Suite

AI augments response teams by analysing vast cyber amount of data, identifying patterns indicative of cyber threats, and facilitating swift and informed decision-making.
Likewise, the Security by Design Life Cycle Suite is designed to support the re-architecture of products as part of such a continuous optimization strategy. By iteratively assessing and adapting to evolving cyber threats, this suite ensures that the organization's Resilience Strategy remains dynamic and effective.
This forward-looking approach empowers the organization to not only respond to current threats but also to proactively anticipate and mitigate emerging risks, thus contributing to the overall cyber resilience maturity of the enterprise (see Figure 3).

CONCLUSIONS

As the digital world continues to evolve at a rapid pace, the imperative for cyber resilience transcends mere optionality, and becomes an indispensable necessity. The products elucidated in this paper furnish indispensable tools for fortifying cyber resilience. Nonetheless, they are accompanied by their own unique set of challenges, ranging from implementation complexities to evolving threat vectors.
By being aware of grappling with these challenges and by properly implementing the recommended strategies, both individuals and organizations can remarkably enhance their readiness to face the relentless flux of the cyber threat landscape. In an epoch in which the inevitability of the next cyber assault looms ominously, it is not a matter of "if" it is to occur, but rather of "when" it will materialize. Embracing cyber resilience emerges as the linchpin for maintaining a competitive edge and for safeguarding the sensitive assets.

Moreover, the significance of a cohesive product ecosystem cannot be overstated in this endeavour. It serves as an indispensable auxiliary force in propelling organizations towards the zenith of cyber resilience. The symbiotic integration of diverse security solutions, threat intelligence platforms, and collaborative tools, amplifies the efficacy of the defence mechanisms. Through seamless interoperability and comprehensive coverage, the product ecosystem empowers organizations to proactively thwart emerging threats and to seamlessly adapt to evolving cyber dynamics.
Thus, in the relentless pursuit of cyber resilience, the cultivation of a robust product ecosystem stands as an indispensable enabler. By harnessing the collective prowess of these innovative solutions and steadfastly facing the attendant challenges, individuals and organizations alike fortify their defences, their resilience, and their future in the increasingly digital world.

Fabio D'Ambrosi: fabio.dambrosi@leonardo.com

REFERENCES

[1] National Institute of Standards and Technology (NIST). (2022). Framework for Improving Critical Infrastructure Cybersecurity Version 2.0. Retrieved from https://www.nist.gov/cyberframework
[2] NIST Cybersecurity Framework. (2022). NIST CSF Version 2.0: Core Functions and Implementation Tiers. Retrieved from https://www.nist.gov/cyberframework/core-functions
[3] Gartner. (2022). DevSecOps: A Framework for Security in a DevOps World. Retrieved from https://www.gartner.com/en/information-technology/glossary/devsecops
[4] National Institute of Standards and Technology (NIST). (2022). Cybersecurity for the Internet of Things. Retrieved from https://www.nist.gov/itl/applied-cybersecurity/nist-cybersecurity-iot-program

Published and Printed by:
Leonardo S.p.A.
Innovation
Piazza Monte Grappa, 4
00195 Roma

The Editorial Team thanks Ombretta Arvigo and Emanuele Angelitti
for serving as the Guest Editors, and Giacomo Troiano, Danilo Defant and Paolo Casanova
or their contribution.

The POLARIS Innovation Journal is an editorial initiative of the Chief Innovation Office.
Other initiatives of the POLARIS Innovation Journal are the Paperbacks and the Lunchtime Webinars.
The Journal invites questions and suggestions from readers.
Contact the Editorial Office at: polaris@leonardo.com

Scan this QR code to access the web version

https://www.leonardo.com/polaris_2024_50/

In compliance with the Leonardo sustainability policies,
and to contribute reducing the environmental footprint of the Company,
the POLARIS Innovation Journal is printed on certified paper (Xerox International Certificate).
The POLARIS Innovation Journal is published biannually.
Issue 50 – April 2024