Resilience of Space Systems: Principles and Practice

8

Regina Peldszus

Contents

Abstract

In view of the increasing complexity of the space environment, resilience has emerged as a pervasive concept in contemporary space security. This chapter provides an overview on the principles and practice of resilience of space systems

R. Peldszus (✉)
Department of Space Situational Awareness, German Aerospace Center (DLR) Space Administration, Bonn, Germany
e-mail: regina.peldszus@dlr.de

K.-U. Schrogl (ed.), *Handbook of Space Security*,
https://doi.org/10.1007/978-3-030-23210-8_87

and operations. It frames the emerging field from two distinct but complementary approaches: mission assurance and deterrence and high reliability and resilience engineering. Drawing on contemporary thinking from civilian and military perspectives, the chapter posits resilience as a distinct yet malleable notion at the intersection of space security and safety and highlights specific areas meriting further engagement for policy makers, systems analysts, and operators.

Introduction

In the past decade, the concept of resilience has come to the fore in contemporary space policy and systems development as a critical quality of space infrastructure and a prerequisite for space security (Pace 2015). As the utilization of the orbital environment transforms, space assets are becoming increasingly exposed to the hazards and dynamics of ever more heterogeneous activity.

Situated within a complex operational domain, space systems are highly complex themselves. Characterized by nonlinear, interdependent interactions and tight coupling, they are prone to incidents or failure (Perrow 2007). Specifically, the bespoke exquisiteness of spacecraft and fleet of spacecraft – the current paradigm of communications, positioning, navigation, timing (PNT), and Earth observation systems – makes them susceptible to internal and external disturbance that includes a hostile physical environment with extreme temperature changes and radiation but may also be posed by operational constraints, mishaps, and, as it is increasingly asserted, the potential of adversary threat.

In view of this "brittleness" or fragility, strategic planners increasingly advocate rendering systems more resilient. (The terms "resilience" and "resiliency" are used synonymously in the relevant body of thought and practice across the sector; for the purpose of this chapter, "resilience" will be used to denote both.) Depending on domain and methodological vantage point, resilience in highly complex large-scale sociotechnical systems refers to the ability to withstand disturbance, bounce back from failure, and continue operations under varying conditions through qualities such as robustness, redundancy, resourcefulness, flexibility, survivability, and contingency planning (Haimes 2009, here 496; Air Force Space Command 2016). Whether articulated as a property or process (cf. sections "Resilient Architecture and Infrastructure: The Mission Assurance and Deterrence Perspective" and "Resilient Operations and Organizations: The High Reliability and Resilience Engineering Perspective"), resilience essentially manifests the *state* of a given system and its subsystems to respond to specific threats, and addressing through physical configuration, operation, and organization is understood as integral to risk management processes (Haimes 2009).

This chapter maps out the conceptual notions of resilience specifically for the space domain. In adopting a distinction parallel to that of security in and from space, focus is placed on resilience *in* space, or of space systems, which here refers to both the space and ground segment.

There is currently no generally agreed nomenclature in the community of practice for defining, describing, implementing, and assessing resilience in space. At the same time, emerging frameworks for the resilience of space systems are not yet widely shared, and their applicability is often tailored to the specific sub-domain they have been conceived to address, i.e., military or civilian system. Charting the notion of "resilience" in the space domain therefore requires casting a wider net in the safety and security sciences and relating already consolidated concepts to emerging formulation in the context of space security.

Two major perspectives on resilience in space currently inform policy making and implementation: on the one hand deterrence and mission assurance and on the other resilience engineering and high reliability organizing. The following first outlines how these strands feature in discussions on resilience in contemporary space security policy and then addresses them in detail with regard to how they theoretically and practically relate to space architecture and infrastructure and organization and operations. Disciplines contributing to resilience in space are then highlighted, and a conclusion suggests issues meriting further attention in the immediate future.

Resilience as Concept in Space Security Policy

As space actors explore future directions in a changing and complex domain, the notion of resilience has lodged itself firmly as an important element in developing space policy. However, despite its pervasive invocation as an end of policy efforts – both to render space systems more resilient and ensure societal resilience through space infrastructure and services – the terminology and approaches to resilience are little consolidated in theory, deconstructed for practical application, or subject of a sustained discourse akin to that for resilience in other domains such as aviation or offshore operations. In the past years, two major conceptual directions have begun to emerge in the USA, Five Eyes community, and Europe, which represent discrete approaches that are mutually complementary.

Resilience for Deterrence in an Emerging Threat Environment: US Perspective

Resilience first surfaced prominently in the US Space Policy of 2010, whose objectives included "increas[ing] assurance and resilience of mission-essential functions" (Arnold and Hays 2013, here 121). The idea was broken down into the development of instruments, structures, and capabilities required for the continuity of space-based services in view of a "degraded, disrupted, or denied space environment," and mechanisms to ensure that requirements for mission assurance and space system resilience would be addressed during acquisition processes for future space capabilities (US National Space Policy 2010, here 9).

In response to disruptive changes in the orbital environment – specifically with regard to new state actors with capabilities that increasingly included a repertoire of technology that could be used for offensive actions – resilience was posited as one of the key approaches to maintaining superiority in space (Pawlikowski et al. 2012): if it were evident to a potential adversary that a system would bounce back from attack, or the damage inflicted would either be recovered swiftly or have limited repercussion on the overall capability afforded through a system or architecture, this would change the calculus of an adversary to attack. The aim was hence a resilient architecture that would be able to "support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, [environmental] conditions, and threats, in spite of hostile action or adverse conditions" (DOD 2012, here 4 and 14). Designing and maintaining a resilient system that would withstand and recover would thus mitigate or deny an adversary the benefit of attack (ibid.). In this sense, resilience formed a fundamental element of layered deterrence (Johnson-Freese 2016).

The US approach to framing and creating taxonomies for resilience in space to this date draws predominantly on the defense vantage point. This is also reflected in the space policies of the Five Eyes community. Here, the focus on architecture and capability subtly shifts to missions or infrastructure but in a similar context of sovereignty, emerging threats, and the terminology of a "congested and contested" domain, whereby resilience would serve as countermeasure against adversarial activities to "disrupt, degrade, or damage" (A New Space Strategy for Canada 2019, here 16; National Space Policy 2015). While not all space policies of the Five Eyes explicitly echo the US concept of resilience in these specific terms, their strategies and reasoning are supported by language to that effect: in placing emphasis on the need for space security, they focus on pillars regarded as contributors to resilience in US space policy, such as international partnerships and Space Situational Awareness (see also section "Disciplines Contributing to Resilience") (cf. the space strategies, respectively policies, of New Zealand and Australia).

The dedicated UK Space Security Policy (2014) further draws on resilience as element of its definition of space security per se. It highlights a dedicated approach with regard to becoming resilient in view of concrete disruptions, both human-made and natural. To this end, the overall goal of resilience of space capabilities and services is diversified into several objectives (ibid., here 4). These include the pursuit of a "proportionate approach to investing in resilience, balancing protective measures with other means [. . .] such as alternative or fallback capabilities" that allow for continued availability of services, with the aim of "enhance[ing] the resilience of essential services [. . .] to the disruption of satellite operations"; and the commitment to "work with [other partners including the US, EU, EU Member States, and ESA] on an integrated approach to security in European space programs [. . .] including infrastructure and systems resilience" (ibid.).

By emphasizing disruption rather than threat and deconstructing resilience in business continuity terms that dovetail with the nomenclature used by a wide range of stakeholders including commercial industry, the UK policy already uses a number of concepts that resonate with a civilian-rooted approach more prevalent in Europe.

Resilience for Critical Infrastructure Protection and Non-dependence: European Perspective

Recent European perspectives on resilience in space reflect US policy to a large degree, albeit on a higher level of abstraction and by situating resilience at the intersection of a multifaceted interpretation of space security, reliability, and safety. They place greater emphasis on space-based systems as critical infrastructure, rather than prominently as means of force projection, space control, and dominance or superiority. Instead, resilience is presented and proposed through a prism of views including civil protection, continuity of services, strategic non-dependence, and autonomy, as necessary measures in response to asymmetric and hybrid threats, as means to foster the synergy of civil and military capabilities or a robust industrial base, and as societal protection from natural hazards (cf. Robinson et al. 2018; ESPI 2018; Pellegrino and Stang 2016, here 8; cf. also ESA's proposed Space Safety program).

National space policies in Europe can be positioned on this spectrum. The French space defense strategy explicitly situates resilience as a central consideration of strategic, operational, and space systems development efforts in view of adversaries' offensive counterspace capabilities (Ministère des Armées 2019). The current German space strategy does not refer to resilience, but the government's overarching security policy deliberations identify resilience of space systems – as critical infrastructure – as fundamental need in the context of hybrid threats (BMVg 2016, pp. 58, 60). Other European space policies do not employ the concept of resilience but draw on compatible concepts, such as reliability, continuity, and access to space, and dedicate considerable attention to laying out specific elements conducive to resilience, such as international partnerships and Space Situational Awareness (cf. the space policies or strategies of Italy, Norway, and Sweden).

On a supranational level, the distinct element of European non-dependence in view of third-party capabilities surfaces, which echoes sovereignty concepts in the US deterrence context. As part of its four strategic goals, the European Union's Space Strategy (European Commission 2016) ascribes to "resilience of critical European space infrastructure" a central role as catalyst to reinforce European autonomy in space access and utilization, by ensuring the "protection" and "integrity" of the flagship programs for navigation and Earth observation, Galileo and Copernicus (here 8–9, cf. also European Defense Action Plan). To this end, and analogous to the USA, the specific measure of consolidating diverse European Space Situational Awareness capabilities is proposed; their current transformation into a dedicated program articulates distinctly civilian terms but accommodates considerable leeway in extending both operational and research and development efforts to a wider range of hazards and threats.

Beyond the specific reference to Space Situational Awareness (SSA) as a driver – and apparent placeholder – for resilience, the concept for resilience is neither fleshed out theoretically in European space policy in further detail nor translated into concrete activities or instruments for assessment and evaluation.

Indeed, the development of a dedicated methodological framework has been pointed out as a necessary element for further discussion (Pellegrino and Stang 2016). Yet, on a higher level in the context of EU foreign and security policy, the idea of resilience has become an overall *leitmotif* and guiding principle in the evolution of shared structures that allow averting external risks and threats (Bendiek 2017, here 14). Similarly, the upcoming NATO space policy can be expected to employ language on resilience, given its increasing awareness of the space domain and an overall stance on addressing hybrid warfare (cf. Prior 2017).

Regardless of the idiosyncratic nuances that are being emphasized in the integration of resilience into space security policy and the level of maturity of the related discourse, there is nascent understanding of the various elements for application in space systems, both in architecture and operations.

Resilient Architecture and Infrastructure: The Mission Assurance and Deterrence Perspective

Extending the scope of policy, a limited but growing body of work exists on deconstructing the concept of resilience into applicable elements for space. One approach, departing from the perspective of assurance and deterrence as outlined previously for US space policy, involves describing discrete measures that can be practically applied in space systems and guide their development.

Resilience as Key Quality of Functional Architecture

In response to the National Security Space Strategy from 2011, and in explicit recognition of the lack of a commonly shared taxonomy to facilitate a discussion on resilience and an approach to measuring it, resilience was fleshed out further through a dedicated taxonomy (OSD 2015). The concept was structured specifically though the lens of mission assurance in the warfighting rather than systems engineering domain, focusing on space-based and ground-based infrastructure. (This was contextualized by highlighting the overall assurance afforded by being able to switch to an alternative domain outside space, which was, however, not subject of the taxonomy effort.) Thus, "Space Domain Mission Assurance" was defined as distinct pillars that flanked resilience between defensive operations and reconstitution (ibid., here 3 and following):

- *Defensive Operations* (disrupting an adversary's ability to target; direct intercept; systematic maneuvering to avoid, confuse, or overwhelm a targeting system; active measures to deceive, degrade, or destroy a targeting system)
- *Reconstitution* (providing backup capacity by launching additional satellites or providing additional ground stations; replenishing parts of a constellations; add new signals or spectrum)

– *Resilience* (an to support "functions necessary for mission success with higher probability, shorter periods of reduced capability . . . in spite of hostile action or adverse conditions")

The taxonomy emphasizes that, rather than resilience per se being the primary goal of an assurance effort, "it is the warfighting mission assurance benefit, derived from resilience, which [it] seek[s] to assure" (ibid., here 2). As a *means* for assurance rather than an inherent overall goal of a system, resilience is understood as an "internally focused characteristic" – a critical quality or property of a capability that helps ensure its continued availability, reliability, and integrity.

Functional Elements of Resilient Architecture

Much of the discussion on mission assurance was initially centered on the concept of disaggregation as one approach to achieve or improve resilience (Air Force Space Command 2016). Disaggregation here meant the "dispersion of space-based missions, functions or sensors across multiple systems" (ibid., here 3). This would entail five disaggregation approaches, including *modular decomposition* within a single system to allow, e.g., individual subcomponent replacement; *functional* disaggregation by distributing sub-missions on separate platforms, including *hosted payloads* on assets of different missions or agencies; *multi-orbit* disaggregation that employs multiple orbital planes; and *multi-domain* disaggregation, whereby space-based and ground-based systems cooperatively or complementarily perform a mission. From a general resilience viewpoint, disaggregation resonates with the fundamental notion of deconcentration of critical or exposed capabilities for target reduction, which constitutes a paramount approach to addressing vulnerabilities of large-scale socio-technical systems (Perrow 2007, here 6 and 261).

However, for the space domain, additional – and partially overlapping – dimensions beyond disaggregation were being explored. Distribution, dispersion, and diversity by leveraging the capabilities of government and commercial stakeholders, increasing the number of platforms, and focusing on hosted payloads and mixed architectures were advocated early on as architectural – and hence also acquisitions-related – responses to the contemporary challenges faced by the traditional class of aggregated, highly integrated assets with long lifetimes (Pawlikowski et al. 2012).

Eventually, the focus of policy makers shifted from disaggregation toward a wider context of space protection after the 2014 Space Strategic Portfolio Review (cf. Johnson-Freese 2016, here 171; McLeod et al. 2016, here xii). Resilience itself was broken down into six characteristic architectural "sub-elements," systematically defining several concepts that had been shown as partially interrelated elements previously (OSD 2015) (Here slightly changed in order of appearance for easier comparison):

– *Disaggregation*, the separation of dissimilar capabilities into separate platforms and payloads, thereby in cases also reducing overall complexity of the system

– *Distribution*, by employing a number of nodes that jointly perform the same function of mission as a single node, allowing for graceful degradation despite failure of a single node
– *Diversification*, by employing different platforms, orbits, systems or actors' capabilities to contribute to the same mission; flexible or adaptable systems
– *Proliferation*, by deploying larger numbers of the same [similar] platforms, payloads, or systems of the same types to perform the same mission
– *Protection*, through active and passive measures including protection from jamming, nuclear hardening, extended maneuverability, internal hosted decoys, onboard countermeasures, onboard/operational event characterization or attribution efforts/instruments
– *Deception*, through measures to confuse or mislead regarding location, capability, operational status, mission type, robustness of system/platform or payload; measures at architectural, operational, or organizational level

While deception was identified explicitly as "a critical element of any space system resilience effort," all elements need not necessarily be present in a single architecture but rather enhance resilience cumulatively or in combination (ibid., here 8).

Practical Measures

A wide range of detailed practical measures can be mapped onto these elements for different levels of space systems. (Note that this selection of practical aspects dovetails with the concepts outlined in the next section.) On the platform level, this may include the hardening and shielding against radiation and kinetic and non-kinetic manipulation; fitting bimodal receivers for different navigation systems or equipping the spacecraft with measures for easier tracking; increased onboard autonomy for measures such as passively safe trajectories during proximity operations; reactive maneuvering in view of another approaching object; and cyber protection to safeguard commanding and telemetry. In the ground segment, there are a number of measures ranging from situating facilities in remote areas for limiting discovery, access, or interference; installing backup facilities; ensuring interoperability with legacy, novel, and partner infrastructure; and putting physical and information security of command and control infrastructure in place (e.g., protecting from mishaps such as severed cables of ground stations during off-site building works, damage or wear of critical equipment through climatic conditions, or compromised mission control software).

Trading Off Resilience and Capability in Architecture

Resilience has been included as a key criterion in the evaluation of alternative space architectures (National Security Space Strategy 2011) and ought to be taken into account at the beginning of the systems planning process as a "critical component to define at system level" (OSD 2015, here 8). Aside from weighing the different elements of resilience against each other, also resilience itself must be traded off with other characteristics of a capability – indeed, since resilience is not understood as a capability itself, resilience and capability must be treated as distinct concepts (Jakhu and Pelton 2017, here 296).

Since in view of resource constraints the benefits of architectural resilience come at a cost, affordability is a key driver in this capability-resilience trade-off (cf. Pawlikowski et al. 2012, here 47). Implementing elements such as distribution or diversification means that other performance aspects of a system or architecture – e.g., sensor coverage, integration times, and procurement cost – may be constrained. These dependencies must be traded against their benefits across the system life cycle and the complete system hierarchy with regard to different threat scenarios (Aerospace 2018).

For want of extensive dedicated metrics, five tentative criteria to assess resilience of a functional architecture include the anticipated level of adversity, functional capability goals of the architecture itself, the risks of not achieving these goals in view of adversities, the severity of functional shortfall, and the duration of downtime that can be tolerated by the mission (DOD 2011).

Resilient Operations and Organizations: The High Reliability and Resilience Engineering Perspective

Once hardware on the ground or in space has been commissioned, changes and modifications to increase the quality of resilience are either infeasible or involve considerable resources. Other system elements are, however, more malleable and may be actively adapted across the life cycle to different extent, including human operators, procedures, or mission rules (McLeod et al. 2016). Next to mission assurance for architecture, a second perspective on resilience hence focuses on operations and organizations rather than infrastructure. Rather than property of a system, resilience here means a continuous pursuit or process, not a characteristic that can be instilled in a system, rather, something that a system is enabled to *perform*.

Normal accident theory (NAT) posits that failure of complex sociotechnical systems in high-risk domains such as space is both inevitable and rare (Perrow 2007). In response to NAT, two proactive fields have formed in safety management across the past decades: high reliability organizing (HRO) and resilience engineering (Haavik et al. 2016). They propose that in view of inherently unsafe systems – or systems exposed to continuous risk – it is in fact the performance of human operators that contributes to safety under varying conditions (Dekker 2012). As they share fundamental terminology with the field of RAMS (Reliability, Availability, Maintainability, Safety) and dependability, and specifically include use cases in both civil and military domains, resilience engineering and high reliability organizing offer an important contemporary lens on aspect of resilience and its context that have not yet matured for the space domain in the mission assurance context.

Resilience Through Sensemaking

Sectors and organizations that are understood through the HRO lens or operate according to HRO principles (i.e., air traffic management, aircraft carriers, utility grids) share fundamental characteristics with space systems. They are highly complex on all levels of the system hierarchy – respectively, nested into systems of systems – with interdependent elements, components, and parts that are tightly coupled and integrated and feature nonlinear interactions. In view of the constraints in the operational environment, they are governed by a high degree of causality, i.e., the laws of physics more so than purely organizational intent, and predominantly face either a physically hostile operating domain (i.e., submarine) or the handling and control of highly hazardous assets or processes (i.e., nuclear power plant). In operations, they rely on the collaboration of distributed actors that may be situated at a distance from the process in a control room environment; in several instances, the system in operation is either highly bespoke or of international significance and sophistication (i.e., a fusion experiment, sample return mission). (In comparison, automotive manufacturing and healthcare environments are also understood as complex undertakings and require a high degree of reliability and continuity but are characterized less by the constraints of physical causality, i.e., when processes come to a halt through a disturbance, the system does not necessarily fail (despite the cost incurred). In contrast, processes in domains such as nuclear power or missile operations require immediate attention and intervention both in routine operations and in view of anomalies in order to avoid irreparable damage or loss.)

Yet, despite tightly coupled processes and constant hazard, highly reliable organizations are able to maintain “continuously safe operations” (Weick and Sutcliffe 2001, here 9). To this end, HROs employ the principle of “collective mindfulness” (ibid., here 9–14). This describes an awareness of ongoing processes by all organizational constituents, combined with an acute understanding of the dependencies and implications of an individual operation or element. Specifically, and in contrast to other types of organizations, HROs operate according to five concrete principles:

- *Preoccupation with failure*, i.e., they cultivate an awareness of small lapses, disturbances, and weak signals; they encourage error reporting and analysis of near misses and foster a culture that challenges complacency and hubris in view of past success.
- *Reluctance to simplify interpretations*, i.e., they deliberately strive for nuanced pictures of a situation and do not rely purely on key indicators; they challenge received wisdom and hear diverse viewpoints.
- *Sensitivity to operations*, i.e., they maintain a situational picture of the “sharp end” (or front line) of operations, which allows continuous adjustments to be made in order to cope with external disturbances.
- *Deference to expertise*, i.e., they foster diverse thinking and an encouragement for decision-making beyond rigid hierarchies by those that are best placed to judge a situation based on their command of the subject matter rather than status or rank.

– *Commitment to resilience*, i.e., maintaining dynamic capabilities for recovery and containment of situations, including flexibility and creative solutions for unexpected problems, but also ensuring continuous supply of fresh resources (i.e., shift personnel) during a crisis or incident.

The final principle can be further understood through the field of resilience engineering. In extending the vantage point and analytical repertoire of HRO, particularly with regard to sensemaking of past, ongoing, and future events, Resilience engineering specifically places emphasis on operator interaction with, and as part of, a system (Leveson 2011; Hollnagel et al. 2008).

Similar to HRO, resilience engineering seeks to understand and leverage the significant part of operations where and how in the face of disturbance the system manages to remain available or "bounces back." (Cf., when looking at a reliability metric of, e.g., 98% in traditional safety management approaches, focus would be directed not only at understanding the 2% of failure cases or incidents, i.e., through failure mode or error analysis, but on the considerable amount of time where "things go right" either in routine or during recovery of anomalies.) Organizational resilience is hence described as the "capability to recognize the boundaries of safe operations . . . to steer back from them in a controlled manner" (Dekker 2005) and as the "ability to anticipate and adapt to potential for surprise and error" (Reason 2008, here 8).

Practically, four key abilities contribute to this adaptation and control, i.e., the overall ability of predicting, planning, and executing (Hollnagel et al. 2008):

– *Factual*, learning from past experience such as incidents in view of devising practical measures to address resilience, knowing what has happened
– *Actual*, responding to actual disturbances and regular and irregular threats, i.e., know what to do, being capable of doing it
– *Critical*, monitoring the system's own performance in order to respond to critical events, i.e., know what to look for and direct attention to the right areas
– *Potential*, anticipating potential disruptions, pressures, and their consequences in the near future, finding out and knowing what to expect

This collective "anticipation of the potential" is a key feature of resilient organizations (Hollnagel et al. 2006). Anticipation focuses on both past and future manifestations and pathways toward failure (Dekker 2012) and aims to make sense of events (i.e., incidents, successful operations). Crucially, it also involves investing resources in the anticipation, adaptation, and growth in response to disruption – both in view of negative stressors and novelty (Reason 2008). The latter part of "growth" represents a critical distinction to other assurance concepts: resilience engineering explicitly includes the possibility that a system is strengthened through meaningfully responding to a continuous barrage of internal and external disturbances. While this potential is usually not formally foreseen in systems planning (e.g., as a performance indicator) and its assessment is not afforded by current safety management tools, in space operations it has been anecdotally evident and crucial to functioning in routine or contingency operations (i.e., creating automated protocols to work around frequently occurring ground station time constraints or outperforming nominal mission life time by ingeniously handling the fuel budget of a spacecraft) or even been assumed as an underlying necessity for missions with high degrees of uncertainty (i.e., devising cutting edge trajectories "on the fly" in response to gradual discovery of targets during special missions).

Resilience Through Performance Variability

Personnel contribute to this quality of adaptation on organizational, team, and individual levels. Practically, they create resilience by adjusting their tasks, inserting buffers or automated routines, using heuristics and double checks, or devising decision-making aids (Dekker 2005, here 12–13) whenever the demands of a situation eclipse predefined rules in an otherwise highly proceduralized domain. This habitual or intentional adjustment is called "performance variability" (Hollnagel et al. 2008).

Rather than being understood as deviation from the norm (i.e., violation of a procedure), performance variability is "normal and necessary" and can be identified by determining the discrepancy of normative and descriptive models of work (ibid.). In space operations, the normative – or designer's – model is described in mission rules, system specifications, formal training manuals, or flight plans as aggregate of procedures. The operator's or "actual" model, however, incorporates also experience after commissioning, as operators "continually test their model against reality," often under time and productivity pressures (Leveson 2011, here 42). Operators may thus determine the change or evolution of the system and its state and the need for subsequent updating of their mental model through varying their performance. These practices require what is termed efficiency-thoroughness trade-off, i.e., where operations have to be compromised in view of resource constraints and increasing demands (Hollnagel et al. 2008).

Practical Measures

Specifically for space operations, some work has explored practical measures for resilience, for both the defense and civilian contexts, by transferring practice from external safety-critical sectors (McLeod et al. 2016; Peldszus 2015). These measures include activities and processes that can be implemented or integrated seamlessly in running operations or carry a comparatively modest cost when juxtaposed with changes in infrastructure, such as:

– *Operational simulation and exercises* using different degrees of fidelity for routine, contingency, and special operations
– *Human performance training* (i.e., communication, situation awareness skills for critical operations)
– *Actionable information and appropriate decision aids*, capturing of shared mental models (i.e., subsystems of an asset)
– Structured, standardized *anomaly resolution* (i.e., according to predefined protocols)

– Centralized, non-punitive *anomaly and near-miss reporting*
– Centralized *operational practice reporting* (incl. recovery and what went “well” in routine)
– Encouraging *smart tacit practice* (i.e., double checks, four-eye principle, informal communication)
– Fostering *culture of openness,* ensuring *availability of resources* to handle serious events
– Building in *slack* or backup plans in processes (including shift planning)

Implementing these measures can be achieved on a spectrum of resource intensity, from updating a rule or procedure, scheduling a short regular review forum, or distributing a familiarization resource to assigning a new position, commissioning a software tool, or rolling out a training campaign. Incentivizing the use of these measures, however, requires an organizational and operational culture that regards resilience as priority (McLeod et al. 2016) and recognizes the critical role of human operators in maintaining resilient operations.

Assessing Resilience in Operations and Organizations

Whether the prerequisites for resilient performance are in fact in place can be evaluated by verifying the deployment and implementation of measures such as those highlighted above. However, whether a complex system really behaves in a resilient manner may arguably only be assessed through a case-by-case appraisal of concrete responses, in view of a specific threat and the particular state of the system at a given time (Haimes 2009). Describing and understanding the functioning of complex systems in routine and contingency may necessitate formal modeling techniques. (These would, for instance, be utilized for architectural trade-offs, cf. previous section.) In order to evaluate resilience, there are, however, additional approaches that include natural language and visual tools.

A structured evaluation of whether and how resilience measures are actually implemented can be performed through methods such as the resilience analysis grid. The method diversifies, in fine granularity, the four key abilities of organizations described earlier (factual, actual, critical, potential) and their requisite resources and processes. As to how fare these measures then impact on operations – and are successful – can be analyzed through modeling methods such as the functional resonance analysis method, which considers the specific conditions, resources, input, and resulting states and can be applied in various operational domains and at various levels of a system.

Disciplines Contributing to Resilience

In addition to the specific measures taken in design and operations to achieve resilience in the mission assurance and reliability context, there are a range of stand-alone fields that contribute to resilience in their own right (see Table 1).

Table 1 High-level elements of resilience in the space domain at a glance

Mission assurance and deterrence	Resilience engineering	High reliability organizing	Contributing disciplines
Disaggregation Distribution Diversification Deception Proliferation Protection	Learning from factual Responding to actual Monitoring critical Anticipating potential	Preoccupation with failure Reluctance to simplify Sensitivity to operation Deference to expertise Commitment to resilience	Space situational awareness Partnerships Information sharing Foresight Transparency and confidence building measures
Architecture	*Operations*	*Organization*	*Governance*

Resilience Through Space Situational Awareness

A key element to remaining resilient from a systems and operational perspective is the ability to understand and act upon risks in the orbital environment in real or near real time through Space Situational Awareness (SSA) (Pellegrino and Stang 2016, here 9). By producing actionable information on the location and behavior of space objects and natural hazards through a general recognized space picture and related services (e.g., collision avoidance), SSA constitutes a fundamental background function that enables the protection of critical services such as navigation and Earth observations. Furthermore, both in the operational and deterrence context, SSA is a prerequisite for resolving certain types of anomalies and for verifying activities that occur in the vicinity of a spacecraft (i.e., rendezvous and proximity operations). Finally, as one of the approaches to mitigating the proliferation of space debris, SSA links directly to the effort of resilience and sustainability of the various orbital regimes per se (McCormick 2013).

A comprehensive understanding of the overall operational environment through SSA benefits considerably from burden sharing. In its reliance on distributed sensor networks for surveillance and tracking, SSA is today viewed as a global undertaking. Efforts to share and fuse information and data from various different sources are currently gaining momentum.

Resilience Through Transparency Measures and Partnerships

The growing heterogeneity and granularity of actors in the space domain both lend itself to – and indeed necessitates – cooperation and transparency. For recovery in operation but also to achieve redundancy already during architectural development, information sharing and cooperation constitute essential means (Jakhu and Pelton 2017, here 269). Resilience considerations specifically encompass the strategic engagement in partnerships with stakeholders in international and domestic government agencies, industry, and academia (Defense Science Board 2017). Allied or partner systems are the subjects of protection efforts, but the forging of closer architectural, operational, and diplomatic ties with allies and partner also constitutes a key resilience measure as such (DOD 2012, here 14). Leveraging a wide range of capabilities facilitates directly the resilience concepts of diversification and distribution (i.e., through payloads hosted on allied or commercial platforms).

Resilience Through Foresight

Enlarging the scale from operational anticipation that is characteristic of highly reliable and resilient enterprises, resilience must build on foresight in order to anticipate wider ranging future challenges (Pawlikowski et al. 2012). Foresight methods are used to explore uncertainties and chart various possible futures (Healey and Hodgkinson 2008). For resilience in space operations, they may range from the systematic cross-disciplinary scanning of risks, developments, and change drivers to the appraisal of low-probability-high-impact events (cf. rare but inevitable failure in normal accident theory) and the crafting of possible scenarios, to the in-depth exploration of specific potential event and the rehearsing of protocols in large-scale tabletop exercises and red teaming (Peldszus 2018). These activities are most frequently undertaken in collaboration with different actors and are employed to inform both operations and strategy. They thus contribute to the facilitation of collaborative decision-making and good governance for space as a resilient domain and global commons.

Conclusion

Despite the current lack of globally shared nomenclature, two salient perspectives have emerged for the principles and practice of resilience for the space domain. They focus on maximizing the continuation and reliability of operations in various conditions or seek to imbue an architecture with qualities that minimize incentives for adversary actions in an evolving threat environment.

Resilience is likely to continue to feature as a key concept in space policy and systems planning. Straddling the fields of space security and reliability, it may inform, enrich, or even galvanize the more traditional security and safety management disciplines. Its incorporation in European policy may, on the one hand, be influenced by US thinking and its current narrow but very applicable focus; on the other hand, the assurance and deterrence context will be enriched by wider use of complementary insights from the civilian domain.

Quite certainly, the onset of the deployment of unprecedentedly large constellations will both exacerbate the dynamics of the operational environment of orbit and offer new challenges and avenues for the notion of resilience. Its apparent ubiquity and perseverance call for deepened engagement in further developing the nascent field. Specifically, there is a need for the cultivation of a broad discourse to facilitate shared nomenclatures, detailed taxonomies, and the development of assessment methods. Here, much insight can be drawn from other high reliability domains: the scholarly and industrial communities of practice hailing from the nuclear, transport, and offshore sectors have been prolific – if not conclusive – in their quest for shared theory and application on resilience. Finally, it will be crucial to examine how notions of resilience are interpreted and addressed in the programs and strategies of other major spacefaring actors (Russia, China, India), whose advanced capabilities may be viewed in the context of both deterrence and high reliability.

References

A New Space Strategy for Canada (2019) Ministry of Innovation, Science and Economic Development, Alberta

Aerospace (2018) Resilience for space systems: concepts, tools and approaches (ATR-2017-02226). Aerospace Corporation, Washington, DC

Air Force Space Command (2016) Resiliency and disaggregated space architectures: a white paper. US Air Force, Colorado Springs

Arnold DC, Hays PL (2013) Strategy and the security space enterprise. In: Sadeh E (ed) (2012) Space strategy in the 21st century: theory and policy. Routledge, London, pp 120–158

Bendiek A (2017) A paradigm shift in the EU's common foreign and security policy: from transformation to resilience. German Institute for International and Security Affairs, Berlin

BMVg (2016) Weissbuch zur Sicherheitspolitik und Zukunft der Bundeswehr. German Federal Ministry of Defence, Berlin

Defense Science Board (2017) Task Force on Defense Strategies for Ensuring the Resilience of National Space Capabilities, March 2017, Office of the Secretary of Defense for Acquisition, Technology and Logistics, Washington D.C.

Dekker S (2005) Ten questions about human error: a new view of human factors and system safety. CRC Press, New York

Dekker S (2012) Just culture: balancing safety and accountability, 2nd edn. Ashgate, Burlington

DOD (2011) Fact sheet: resilience of space capabilities. US Department of Defense, Washington, DC

DOD (2012) Directive 3100.10: space policy (update 2016). US Department of Defense, Washington, DC

ESPI (2018) Security in outer space: rising stakes in Europe. European Space Policy Institute, Vienna

European Commission (2016) A space strategy for Europe, COM (2016) 705. European Commission, Brussels

Haavik TK, Antonsen S, Rosness R, Hale A (2016) HRO and RE: a pragmatic perspective. Saf Sci. https://doi.org/10.1016/j.ssci.2016.08.010

Haimes YY (2009) On the definition of resilience in systems. Risk Anal 29(4):498–501

Healey MP, Hodgkinson GP (2008) Troubling futures: scenarios and scenario planning for organizational decision making. In: Hodgkinson GP, Starbuck WH (eds) The Oxford handbook of organizational decision making. Oxford University Press, Oxford, pp 565–585

Hollnagel E, Woods DD, Leveson NG (2006) Resilience engineering: concepts and precepts. Ashgate, Burlington

Hollnagel E, Nemeth CP, Dekker S (eds) (2008) Remaining sensitive to the possibility of failure. Resilience engineering perspectives, vol 1. Ashgate, Burlington

Jakhu RS, Pelton JN (2017) Global space governance: an international study. Springer, New York

Johnson-Freese J (2016) Space warfare in the 21st century: arming the heavens. Routledge, New York

Leveson NG (2011) Engineering a safer world: systems thinking applied to safety. MIT Press, Cambridge, MA

McCormick PK (2013) Space debris: conjunction opportunities and opportunities for international cooperation. Sci Public Policy 40(6):801–813

McLeod G, Nacouzi G, Dreyer P, Eisman M, Hura M, Langeland KS, Manheim D (2016) Enhancing space resilience through non-material means. RAND Corporation, Santa Monica

Ministère des Armées (2019) Stratégie Spatiale de Défense: Rapport du groupe de travail ≪ Espace ≫, Ministere des Armees, Paris

NSSS (2011) National security space strategy: unclassified summary. US Department of Defense and Office of the Director of National Intelligence, Washington, DC

OSD (2015) Space domain mission assurance: a resilience taxonomy. Office of the Assistance Secretary of Defense for Homeland Defense & Global Security, Washington, DC

Pace S (2015) Security in space. Space Policy 33(2):51–55

Parly F (2018) Intervention de Florence Parly, ministre des Armées: Espace et défense, 7 September 2018, CNES, Toulouse. https://www.defense.gouv.fr/actualites/articles/direct-florence-parly-s-exprime-sur-les-enjeux-de-l-espace-pour-la-defense. Accessed 22 Jan 2018

Pawlikowski E, Loverro D, Cristler T (2012) Space: disruptive challenges, new opportunities and new strategies. Strateg Stud Q 6(1):27–54

Peldszus R (2015) The Human Element and System Resilience at the European Space Operations Centre, AMCO-TN-0006 and AMCO-TN-00011 (Internal Reports), ESOC, Darmstadt

Peldszus R (2018) Foresight methods for multilateral collaboration in space situational awareness (SSA) policy and operations. J Space Saf Eng 5(2):115–120

Pellegrino M, Stang G (2016) Space security for Europe. EUISS report no. 29, July 2016. EU Institute for Security Studies, Paris

Perrow C (2007) The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters. Princeton University Press, Princeton/Oxford

Prior T (2017) NATO: pushing the boundaries for resilience. CSS analyses in security policy, CSS report no. 213. Center for Security Studies, Zurich

Reason J (2008) The human contribution: unsafe acts, accidents and heroic recoveries. Ashgate, Farnham

Robinson J, Šmuclerová M, Degl'Innocenti L, Perrichon L, Pražák J (2018) Europe's preparedness to respond to space hybrid operations. PSSI report July 2018. Prague Security Studies Institute, Prague

UK National Space Policy (2015) HM Government, London

UK Space Security Policy (2014) HM Government, London

US National Space Policy (2010) Office of the President of the United States, Washington, DC

Weick KE, Sutcliffe KM (2001) Managing the unexpected: assuring high performance in an age of complexity. Wiley, New York