The Road to Resilience –

Critical Space Infrastructures and Space Security

Resilience is the ability of a complex system, such as a human society of varying sizes, to withstand the harmful impact of unexpected negative events while mitigating their damage and enabling the rapid resumption of a normal state of functioning. It is a deeply complex concept, related to other concepts such as robustness, flexibility and rapidity[1]. Some authors have tried to make sense of the concept by connecting it to three underlying capacities a complex system can exhibit – an absorptive, restorative and adaptive capacity[2]. Yet others try to identify principles of resilience as a sort of roadmap towards developing this abstract quality in an indirect fashion. Stig Johnsen[3] defined seven such principles of resilience, easily understood in the context of resilience of complex, technical and human, systems-of-systems – graceful decline, management of margins, common mental modes, redundancy, flexibility, complexity reduction and deemphasizing couplings between system components.

What is certain from the increasing emphasis on resilience and the research that has already occurred is that resilience is deeply circumstantial and arises or falls from the characteristics of the system in question. Pre-globalized, low technology economies have a certain resilience profile that is completely different from that of an advanced, globalized economy. An autarkic nation such as North Korea certainly seemed less affected by the 2008 Global Financial Crises than prosperous and open nations such as the Unites States, but one finds it hard to envy the North Koreans for their poverty. To describe resilience in 2050, it is crucial to describe the societies in that era, especially with respect to their underlying economic, social and political functioning. Whether or not it comes to pass, the trend seems to be for all societies to want to increase their prosperity. The underlying framework of such development is an evolving system of infrastructures, both technical and organizational, concentrated and diffuse, ranging from pipelines and power plants to agricultural and water systems, health and education systems, as well as finance.

These infrastructures work in concert, meaning that they are interdependent and their proper functioning as a whole is required for a multilaterally developed system. This makes them critical to the wellbeing of a system-of-systems such as a human society. The complexity of the inter-connections and the degree of dependence on these systems engender an intractable problem – to grow, one needs to develop critical infrastructure. The more you have, the more exposed you are to certain threats and vulnerabilities, both known and unknown, which can have dire repercussions through cascading failures within the systems. Take the example of a city, the undisputed engine of growth in the current development model, featuring a concentration of critical infrastructures. There were cases where the summer consumption overwhelmed the electricity grid and resulted in the interruption of supply for a certain period of time. This leads to cascading disruptions in many infrastructure systems – public transport (underground), food and water systems (storage, distribution, waste management), financial, educational, health systems and, last but not least, in administrative capacity, which is considered a critical infrastructure under the European Union Programme for Critical Infrastructure Protection (EPCIP). Public order is affected, especially if the situation continues, as rioting and looting take place and the security services are unable to properly coordinate an effective response or simply attend to all of the hotspots.

It is in relation to these critical infrastructures (CI) that the concept of resilience has become a fixture in security and policy discussions. Economists used to speak of capital accumulation in general terms as a basis for economic development, but we can now speak also of infrastructure accumulation as a precondition for development, with criticality as a side effect. The paradox is that a society will only be as prosperous and as safe as its critical infrastructures will allow, thus setting both lower and upper bounds to prosperity by encumbering it with the weight of the security perspective.

It is understood that the relentless drive towards greater efficiency and economic growth often outstrips the capacity of the security apparatus (both formal and emergent) to keep up with emergent threats and vulnerabilities. Methods of inventory management such as “just in time” which minimize acquisitions and storage costs by relying on clockwork delivery schedules within

global chains of production illustrate this penumbra of incompatibility between growth/efficiency and resilience. Security standards may be developed and imposed, or voluntarily adopted by private actors for the sake of minimising upheavals, but the truth remains that resilience is, to a certain extent, anti-efficient if society ends up being critically dependent on the gains made with each new degree of efficiency.

Limiting growth itself is unlikely as a conscious policy, since it is deeply impolitic and would be regarded as being regressive and on the wrong side of history. To borrow a phrase from American political conservatism, it is akin to "standing athwart History, yelling stop". New methods have to be developed to maintain resilience, because achieving it is nigh impossible in an ever-evolving infrastructure landscape, where regional criticality is replaced by global criticality whose handling outstrips the jurisdiction, resources and, ultimately, vision of most security actors. It is in this gap that the capabilities of space systems have come to play an important role. Future historians might debate which role came first, that of adjuvant to resilience issues or detractor from it, but the rapid rise in the use of space capabilities is a telling indicator of their significant advantages.

Space systems have become a key enabler of a wide range of applications for billions of beneficiaries, if not consumers. Satellites and satellite constellations provide multiple services, such as communications, Earth Observation and remote sensing, navigation, positioning and timing. These capabilities supplement or complement those of critical terrestrial infrastructures, enhancing them. Just to give an example, global transport systems today are increasingly dependent on Global Navigation Satellite Systems (GNSS). Even the banking system depends on the atomic clocks of GNSS for timestamping innumerable transactions, while the electricity grids depends on them for synchronising increasingly complex systems of energy producers and consumers.

Crucially, from the perspective of resilience, space systems have become an upper layer of command, control and coordination capabilities which are spreading, due to technical prowess, efficiency and cost effectiveness, to many critical infrastructure systems. This engenders a critical dependency on these capabilities which leads to the conclusion that space systems are themselves

becoming critical infrastructures and therefore, not just part of a solution, but part of the problem. The European Union and National authorities (overwhelmingly those of the most developed states, but also the strongest of the emerging world), which are the main drivers of Critical Infrastructure Protection (CIP) efforts and research, are increasingly coming around to this development and scrambling to update their mental modes, organizations and documents of reference to reflect this new variable.

It is true that, for instance, weather monitoring has become an extraordinary tool in the hands of emergency and crisis situation management, not just for everyday economic activities (agriculture, transport etc). Space systems have become a boon for localized disaster management, but it is this proficiency which has led to a dependency that spawns new threats and vulnerabilities, given the challenging and complex security environment in which space systems have to operate.

The year 2050 is liable to offer more of the same, featuring not some resolution to the problem of ensuring resilience, but an eternal tightrope balancing act to handle existing security issues by deploying capabilities which, in turn, may create new issues, all the while hoping that the security calculus will turn out to have been 'in the black'. We can get a glimpse of the future today since, as science fiction author William Gibson quipped, 'the future is already here, it is just not evenly distributed'. The largest economies, at least in per capita terms, are also the most technologically advanced and therefore the most endowed with critical infrastructures. These countries are also the progenitors and heaviest users of space capabilities. The contrast is not only with poor, underdeveloped nations, which have themselves become the marginal space services consumers under the aegis of international development projects which seek to bypass elements of local critical infrastructure development. Developments such as skipping the construction of landlines for communications and going straight to mobile communications or using remote sensing for sustainable water use were unavailable to Western nations during their incremental development at the technological and economic frontier.

The contrast is also with the past, which shows a clear progression towards greater use of space systems. The militaries of developed nations, especially that of the United States, have been

at the forefront of developing space capabilities which were then adapted for civilian use. Among them is the first global positioning and navigation system (GPS), which is still a project of American Department of Defence (DOD). Consequently, military thinking in space security issues is still among the most advanced, as critical dependency issues manifested earlier and have been under scrutiny for a longer period of time. The United States owns 152 of the known existing 270 military satellites[4], as well as countless other civilian satellites with implicit dual use capabilities (which are most of them). Just to highlight the degree to which the military is a trailblazer for space dependencies, a single Global Hawk drone that flies over the Middle East consumes more transmission bandwidth than was consumed during the entire Gulf War in 1991, and 90 per cent of the US military traffic passes through civilian satellites, many with a private owner, and not through systems constructed to be resilient to various means of interrupting their functioning. Furthermore, 68 per cent of American ammunition used in Iraq was guided through satellites, while only 10 per cent was guided in the same manner during the Gulf War. Already, American strategists have stopped talking about the 'fog of war' and have started talking about the 'cloud of electrons' and about the fact that space systems are an 'Achilles' heel' for the US[5].

Military exercises like Army After Next, Navy Global, Air Force Global Engagement, Space Game 2, Schriever 1 and 2 and DEADSATS, confirmed the fact that 'politicians, economists and company chiefs ignored the fact that space losses can affect national, economic and social security, not just in the United States, but also in the entire world'. American experts concluded that even major military powers could be 'taken hostage by the unknown elements of a new type of war'. Another military exercise, 'Pacific Vision', demonstrated the vulnerability of commercial communications satellites on which they depend. Referring to the anti-satellite weaponry (ASAT) test of China from 2007, General Harnel from the Space and Missile Systems Centre declared that 'losing asymmetric advantage in space will regress the American war machine from the informational age to the industrial age' in favour of the adversary[6].

Therefore, the writing has been on the wall for quite a long time, nearly a generation now. The use of space systems is on a natural growth path and the trends will be maintained in 2050.

Space capabilities will be a crucial enhancer for the growth and development of already advanced nations, and a key component for the catch-up growth of the less developed nations. Space capabilities will also be a crucial component of the resilience capacity of nations, while undermining it at other levels. Dependencies will abound, not just of the first order, but also at secondary and tertiary levels, where cascading disruptions will challenge even countries that thought themselves beneath reliance on space systems.

Crucially, one does not have to be a participant in a new 'space race' to be dependent on space systems, as many smaller developing or developed nations are full-fledged users of space services without ever having launched a satellite. Such situations underline the complexity of resilience in the age of the space systems, since they lead to subtle political risks (or limitations on security efforts) resulting from a dependence on infrastructures that are not under their jurisdiction, being owned by foreign companies under the sovereignty of other states and subject to other laws. The pseudo-military nature of GPS is a very good illustration of how a critical dependency has been formed at global levels on an infrastructure under an authority which can arbitrarily terminate or degrade its service to certain categories of users, such as civilians of allied states.

We can posit not just a trend in the growth of the use (and dependency on) space systems, but an acceleration based on factors which seem likely to materialize today, reducing the barriers of access to space:

- A projected lowering of the launch costs, given greater competition in the field;
- A lowering of new asset cost, through technological development, economies of scale, new design philosophies (modular satellites, nanosatellite swarms);
- A lowering of costs such as insurance and financing, through a better understanding of the security environment and the gradual build-up of a better framework of commercial exploitation of space under more predictable conditions (global governance, international organizations dedicated to administering the global space commons, international legislation and an adaptation of existing commercial law and customs to space, including for potential liability);

- New business models for access to space, including the ESA's Copernicus Programme, which features an open-source data model for the observations of the Sentinel satellites.

Of course, this simply complicates the issue of whether the trend in the space services sector is towards greater resilience with regards to critical dependencies on space systems through an expansion of the capacity of the sector, or whether there will be such a rise in consumption that it will erode any possible capacity reserves for the provision of space services (possibly even goods, in the future), reducing resilience.

We mentioned the trade-off that is taking place through the advancement of the space services sector, where increased and more efficient economic and security governance activities also register a corresponding increase in exposure to new types of risks, vulnerabilities and threats, resulting from these systems. The security profile of critical space infrastructure is markedly different from that of the average National CI.

For one, space itself is a highly international environment, a sort of global commons, where security actors are hamstrung by jurisdictional issues, cross-dependencies that render geographical and territorial borders irrelevant and gaps in the international framework for the governance of such environments, which is apparent in the growing issue and threat of space debris.

Due to barriers of access to space and the types of services being provided, the number of active space systems is very small relative to the extraordinary number of consumers and other beneficiaries. The Union of Concerned Scientists maintains a database of known satellites by ownership, orbit, type of activity and other metrics[7]:

Satellite Quick Facts *(includes launches through 31.08.2015)*			
Total number of operating satellites: 1305			
United States: 549	Russia: 131	China: 142	Other: 483
LEO: 696	MEO: 87	Elliptical: 41	GEO: 481

Total number of U.S. satellites: 549			
Civil: 21	Commercial: 250	Government: 126	Military: 152

Because of weight limitations and the needs to provide specialised services, most satellites are built for specific tasks. Therefore, the degree of interoperability and substitution which can cushion the effects of a disruption in services is very small. Constellations exist to provide global coverage and the amount of built-in redundancy is very small, since every new asset is leveraged for maximum economic gain. The trend has been for private companies to assume greater importance in critical space infrastructures, just as in terrestrial CI, which obviously produces tension between the profit motive and the requirements of security and prudence. Consequently, the systems featuring the most redundancy are the government sponsored constellations, such as the various GNSS systems, which feature back-up satellites to prevent degradation of service in case of asset loss. The Galileo GNSS features an interesting degree of interoperability with the American GPS system and the Russian GLONASS, while all major players also use ground-based amplification stations to improve the accuracy of positioning.

Coupled with the high risk of spontaneous malfunction in a very hostile environment saturated with radiation and other hazards, in which repairs are, most often, impractical and replacement takes a long time, this means that space systems are, at the same time, critical assets, critically undermanned and critically threatened. Other specific vulnerabilities are related to their exposure to human interference:

- Their orbital paths are well known and predictable, as well as clustered in the most profitable orbital bands;
- Their paths may take them above areas inhabited by hostile elements;
- According to a Rand Corporation report[8], they make enticing targets, especially for non-state actors who are insensitive to the logic of mutual deterrence that inhibits nation-states from attacking space assets on which their might even be a mutual dependence. Their

disruption or destruction appears to be a crime without casualties, but with extraordinary economic costs beyond the simple cost of replacement and can be more attractive in a political sense;

- The means to attack them are increasingly at the disposal of non-state actors or rogue states and are also very diverse, ranging from kinetic weaponry to cyber-attacks and from signal jamming to laser blinding. Some of these attacks can have highly specific outcomes – stealing data, faking data, temporarily blinding a satellite to inhibit surveillance, inhibiting communications, and are not just the province of terrorists and rogue states, but also of potential organized crime elements;
- Certain means of attack are especially attractive, since they provide an extraordinary difference between costs of attacks (including failures) and the value of a successful strike. Having a laptop with an Internet connection and an operator with specific skills is a very low threshold for implementing an attack that debilitates world markets or robs decision makers of certain capabilities at critical junctures (during an emergency situation, for instance). Jamming, especially at the ground stations, is also a low-cost and low sophistication approach, with increasing availability of off-the-shelf equipment for such operations.

Space systems also face two specific threats – space debris and space weather, the latter of which can also impact terrestrial SCI, especially in energy and communications.

Most human activity is concentrated in a thin layer of orbital space surrounding the Earth, where decades of launches, accidents, collisions and carelessness have produced hundreds of thousands of objects larger than a centimetre hurtling through space at 8 km/s. Orbital space is one of the least regenerative environments known to man, and there have been fears, such as the Kessler Syndrome proposition[9], of debris density becoming so high that one final collision produces a cascade effect rendering Low Earth Orbit into a dangerous minefield. In February 2009 an American commercial satellite collided with a Russian military one at the speed of 11.7 km/s. The number of traceable debris generated by the incident numbered over 2,000, with thousands more too

small for tracing. It was the first random collision between satellites at hyper speeds, although there had been other incidents in the past. The Russian satellite was a 950 kg, nuclear-powered military satellite called Kosmos-225, which was launched in 1993 and deactivated in 1995. The American one weighed 560 kg, had been active since 1997, and was link number 33 in the Iridium Corporation communication network which contained 66 units. A representative from Iridium stated that they received 400 weekly close proximity warnings, issued when an Iridium satellite is within 5 km of another satellite, and Iridium 33 was scheduled to bypass the Russian relic by only 560 metres[10].

ASAT weaponry tests have also been a source of space debris and, in case of conflict, could provide the trigger for a Kessler Syndrome situation. For instance, the ASAT test run by China on the 750 kilogram FengYun-1C at 865 kilometres altitude on 11 January 2007 increased the number of monitored orbit debris by 12 per cent - NORAD has detected over 2,000 new objects the size of golf balls or larger, with the likelihood of 100,000 smaller objects, equally dangerous[11].

Unlike extreme Earth weather, which disproportionately impacts the populations of poor countries, space weather impacts rich countries above all others, since they are the biggest consumers of space services and they derive the greatest economic added value from employing them in the economy. Space weather is primarily made up of the high speed ejections of plasma from the Sun, which experiences periodic solar flares, but also incorporates other sources of radiation and charged particles. There has never been a truly destructive solar flare event, because only recently have we become vulnerable to them. We have the example of the Carrington event which, in 1859, led to auroras manifesting at the Equator, measurement devices becoming erratic and world telegraph networks being heavily damaged. Our vulnerability, despite never being severely tested, has grown with each passing year, to the extent to which we can safely say that it has become an existential threat for developed societies. One of the largest modern instances, on 13-14 September 1989, led to a loss of contact with numerous space assets for over a week and left six million inhabitants of the Canadian province of Quebec without electricity for several hours, and many planes grounded or rerouted[12]. Solar weather can also lead to disruptions of services and

significant damage at terrestrial level. In 2003, during the "Halloween storm"[13] which was another peak of solar activity, alongside power disruptions on the ground, orbital activity was seriously affected – 59 per cent of scientific missions were interrupted, astronauts had to take refuge in specially shielded areas of the ISS, and a number of satellites were lost[14].

In case of a modern Carrington event, the US National Academy of Sciences (NAS) estimated damages at 2 trillion dollars in the first year for the US alone, and recovery times between four and ten years[15], without also counting damages to electricity grids in Europe, lost economic opportunity and so on. Other key terrestrial infrastructures can also be disrupted, mostly as a result of the loss of electricity and communications. Future events could exploit weak links in infrastructure systems to inflict even greater damage, with the NAS estimating that, due to vulnerable and aging transformer stations, over 130 million consumers in the US alone would be deprived electricity for more than a few hours[16]. Space systems also play a vital role in researching these phenomena and warning against them.

Extrapolating these trends to 2050, mindful of potential technological breakthroughs, allows us to get a picture of how space systems will both add to and detract from the goal of ensuring societal resilience. By then, every country developed to at least the economic and technological level of the early 21st century will have registered a critical dependence on space systems, especially for emerging countries which have leapfrogged over technological stages to directly utilize space services. Countries will be richer and safer from a host of potential disasters and disruptions through ubiquitous surveillance, information gathering and coordination at accessible price levels through space systems.

However, the world will be at the peak of its vulnerability to space debris and space weather phenomena, while a cautious détente between spacefaring nations is maintained by crosscutting issues of dependence, if not on the same systems, then at least on the health and safety of the "global commons in space". This will also be a time of opportunity for violent non-state actors looking to disrupt world affairs, though it is arguable that the systems will have become more resilient in themselves regardless of the financial and market impact of temporary disruptions, based

on the psychological effects of uncertainty which are beyond the security decision makers' ability to affect.

The main barrier to such a resilient world in many more respects than today is the task of creating a global governance framework with real powers to regulate space activities in a way that increases resilience. The current framework, based on voluntary associations between space agencies and other actors, as well as voluntary adoption of technical standards without power and authority to penalise actors who deviate from these norms, is woefully lacking. The United Nations' Committee on the Peaceful Uses of Outer Space has been developing such technical standards, but with little power of enforcement. Different treaties are supported by a mosaic of nations in various stages of adopting them, while other treaties lack the support of the most powerful space players who are holding out for a framework that is to their specific advantage. Organisations such as the International Telecommunications Union, which regulates and assigns communication frequency bands to avoid "frequency fratricide" between nearby satellites (which is also a potential ASAT weapon)[17] shows that the "orbital commons" can be adequately regulated.

Going forward, an international governance framework conducive to such resilience would:

- Regulate the production and disposal of new space debris;
- Regulate oversaturated orbital bands, preferably through market mechanisms;
- Incentivize the development and application of methods for clearing up orbital debris;
- Promote the adoption of resilient satellite design, taking advantage of new technologies and lower costs of launch (for shielding) to increase lifespan and decrease failures, as well as ensure the highest possible extent of interoperability;
- Develop a multi-stakeholder model of governance, focused especially on co-opting private actors (who will own the bulk of future satellites) in a security conscious process while addressing their needs for an environment more conducive to commercial exploitation;
- Another target should be non-spacefaring nations, who must nevertheless take space security into account for their Critical Infrastructure Protection strategies and activities. This is

especially important since, in an interconnected world, one weak link also undermines the other countries through cascading disruption, even though they may have thought themselves adequately protected from threats;

- A comprehensive effort at disseminating knowledge, best practices and critical technologies and standards, while co-opting as many members as possible into arrangement such as early warning networks and rapid intervention initiatives;
- A focus on terrestrial infrastructure as well, and hardening it against threats such as space weather phenomena, a process which involves not only investments and upgrades on the ground, but the use of space systems for adequately early warning and research.

In the end, space systems are a critical tool in negotiating the often conflicted relationship between economic development and security concerns. Their use enables us to achieve a greater measure of resilience towards certain kinds of disasters than ever before, but at the cost of exposure to new threats. By 2050, we will have not only integrated them into existing and future Critical Infrastructure Protection frameworks at National, European and global levels, but we will have also gone through a number of challenges that will have strengthened our resilience. Experts studying the various cases of low intensity space weather phenomena that have, nonetheless, produced damages, have remarked on how they represented stress tests of existing infrastructure and wake-up calls for the need to address these issues. As a result, the various examples we have had of space system disruption and destruction have been a positive incentive for security conscious development. This relates to the concept of "anti-fragility"[18], where repeated low level crises actually strengthen a system against a major threat which could have otherwise destroyed the system entirely. The philosophy is now being applied to Critical Infrastructure Protection and to space security issues.

By 2050, the effects of past incidents will have already spawned a more resilient society, but it will have become obvious that the road to resilience extends much farther into the future, as long as societies continue to develop and avoid stagnation. Resilience, in this respect, is less of a destination for security experts and decision makers, and more of a constant journey.

[1] Per Hokstad, Ingrid B. Utne, Jørn Vatn, *Risk and Interdependencies in Critical Infrastructures*, (Springer Series in Reliability Engineering, Springer, Trondheim, Norway, 2012, ISBN 978-1-4471-4661-2), pg 16-18
[2] E. Vugrin, D. Wahren şi M. Ehlen, 'A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane', paper presented at Sandia National Labs, US, during the 6th Global Congress of Security Processes, March 2010
[3] Stig Johnsen, 'Resilience in risk analysis and risk assessment' in Tyler Moore and Sujeet Shenoi *Critical Infrastructure Protection IV - Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection* (Washington DC, 15-17 March 2010, IFIP Advances in Information and Communication Technology 311, Springer 2010, ISBN- 13 978-3-642-16805-5), pg 211-27
[4] Union of Concerned Scientists open-source satellite database statistics, <http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.Vg0BUCvkVTB> accessed 30.09.2015
[5] Ian Easton, 'The Great Game in Space - China's Evolving ASAT Weapons Programs and Their Implications for Future U.S. Strategy', pg. 8, published by the Project 2049 Institute, <http://project2049.net/documents/china_asat_weapons_the_great_game_in_space.pdf> accessed 15.09.2015
[6] Ibid.
[7] Union of Concerned Scientists open-source satellite database statistics, <http://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database.html#.Vg0BUCvkVTB> accessed 30.09.2015
[8] Interview with Donald Kessler, http://webpages.charter.net/dkessler/files/KesSym.html
[9] Austin Long, 'Deterrence – From Cold War to Long War', Rand Corporation, published 2008, <http://www.rand.org/pubs/monographs/2008/RAND_MG636.pdf> accessed 09.09.2015
[10] Brian Weeden, 'Billiards in Space', published 23 February 2009 by The Space Review, <http://www.thespacereview.com/article/1314/1> accessed 20.09.2015
[11] Carmen Pardini and Luciano Anselmo, 'Evolution of the debris cloud generated by the FengYun-1C fragmentation event', published by Space Flight Dynamics Laboratory (Istituto di Scienza e Tecnologie dell'Informazione "Alessandro Faedo", Pisa, Italy, 2007), <http://issfd.org/ISSFD_2007/10-4.pdf> accessed 15.09.2015
[12] Royal Academy of Engineering, *Extreme space weather: impacts on engineered systems and infrastructure*, (London, 2013, ISBN 1-903496-95-0), pg. 18, <www.raeng.org.uk/spaceweather> accessed 19.09.2015
[13] M. Weaver, W. Murtagh, et al., *Halloween Space Weather Storms of 2003*, NOAA Technical Memorandum, (OAR SEC -88, NOAA, 2004)
[14]Yousaf M. Butt, 'The EMP threat: fact, fiction and response', published 1 February 2010 by The Space Review, <http://www.thespacereview.com/article/1553/1> accessed 10.09.2015
[15] National Research Council, *Severe Space Weather Events: Understanding their Economic and Societal Impact*, Workshop Report (Washington DC, 2008) <http://lasp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf> page 4, accessed 23.09.2015
[16]Ibid, pages 3 and 78
[17] Centre for Developments, Concepts and Doctrine, *Space: Dependencies, Vulnerabilities and Threats*, (United Kingdom Ministry of Defence, Shrivenham, 2012), section 4-8
[18] John Johnson, Adrian Gheorghe, 'Antifragility Analysis and Measurement Framework for Systems of Systems', published in *International Journal of Disaster Risk Sciences* (Volume 4, No. 4, 2013) pg 159–68