Game Changer "Cyber" – Towards New Economics of Space?

Ralph D. Thiele

June 2019

Summary

Satellite Communications (SATCOM) can be expected to be a crucial backbone of evolving global communications networks. As access to space gets cheaper, satellites are becoming mass-produced devices. The unhindered access to – and freedom to operate in – space is of vital importance to nations and international organisations, such as NATO and the European Union. Navigation and weather monitoring, communications and financial networks, military and intelligence systems – all of these and more have components in the space domain. Opponents understand this well and have been preparing hybrid measures for downgrading C4I. Cyber threats to space systems by state/non state actors are rapidly developing. Innovation in space technologies has increasingly been driven by security and defence needs. Consequently, the tasks of securing outer space and cyberspace are converging. There is a premium on disruptive and game-changing technologies that are autonomous, reconfigurable, agile and adaptable. Governments, commercial customers and industry should all prepare themselves for new business models and the new economics of space as there is substantial change coming up. Cyber is the driver.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

1. Hybrid & Disruptive

Hybrid threats and disruptive technologies are shaping a diverse, and fast-developing strategic environment in which an increasing number of relevant actors build their security strategies on the rule of force. A clear and memorable visualisation of the term hybrid threats occurred in the Russian use of little green men. These were soldiers in unmarked green army uniforms, carrying modern Russian military weapons and equipment that appeared during the Ukrainian crisis of 2014. These and other hybrid threats have blurred the traditionally understood division between conventional and unconventional threats. They combine: high-tech and low-tech weaponry; new strategies and tactics; a wide and confusing array of state and non-state combatants; overlapping political, criminal, economic and terroristic methods and agendas; as well as multiple informational techniques, including traditional and social media.

Technological upheavals suggest that the portfolio of hybrid hazards will rapidly expand. Computers are becoming faster and ubiquitous. Other fundamental breakthroughs include robotics, nano- and biotechnology, artificial intelligence, sensor technology and 5G. Machines are getting smaller and more powerful every day. In the increasingly developed knowledge society, knowledge proliferates not only legally, but very often also through systematic theft of intellectual property. Communication technologies are enabling this development.

Data is growing exponentially. It must be transmitted between multitudes of devices. Satellite Communications (SATCOM) can be expected to be a crucial backbone of evolving global communications networks. As access to space gets cheaper, satellites are becoming more like mobile phones – mass-produced devices that are used for a few years and then replaced. Commercial space companies are already fielding hundreds of small, cheap satellites. Soon, there will be thousands of such satellites, providing eyes and ears over the entire world to include low earth orbit nano-satellites for missile warning, intelligence, surveillance, reconnaissance, navigation and communications.

Cyber has emerged as the absolute and unsurpassed enabler of hybrid threats posed by government agencies and non-state actors. Some are seeing cyber as a discipline in its own right. Yet, its power is hybrid and it's driven by information. Anyway, the time when cyber was simply an emerging capability that needed to be exploited is long gone. Today cyber has become a game changer in multiple domains. It has evolved into a global domain consisting of the interdependent networks of information technology infrastructures and resident data. This includes the internet, telecommunications networks, and computer systems. Equally, it has significant influence on other domains, such as land, air, sea, and space. Space superiority has become indispensable in achieving global awareness, information superiority on the battlefield, deterrence of potential conflict, and combat effectiveness.[1]

The unhindered access to – and freedom to operate in – space is of vital importance to nations and international organisations, such as NATO and the European Union. Navigation and weather monitoring, communications and financial networks, military and intelligence systems – all of these and more have components in the space domain. Opponents understand this well. Space has become their centre of gravity for downgrading C4I. Against this backdrop, one of the most challenging of potential scenarios – actually one currently confronting NATO and the European Union – is an opponent's ability to establish Anti-Access/Area Denial (A2/AD)

[1] EDA. 2018 CDP Revision. The EU Capability Development Priorities. Brussels. Pg. 9. https://www.eda.europa.eu/docs/default-source/eda-publications/eda-brochure-cdp

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

postures, i.e. an opponent's ability to counter one's own power projection, blocking freedom of manoeuvre in key areas.

Cyber threats to space systems by state/non state actors are rapidly developing thus enabling A2AD. There is a wide range of motivations – socio economic, military, terrorist, etc. The complexity of technology makes attribution difficult. Hybrid threats, such as spying or interrupting services, add to the given complexity. A grey zone of predominantly covert aggression has emerged. Given that there are few distributed technological systems that do not rely on satellites for some vital piece of their functionality, the importance of space assets and retaining the confidentiality, integrity, and availability of the information that they carry cannot be over-stated. It is, thus, evidently of concern that space assets have not been properly protected against cyber and hybrid attacks.

2. NEO & MEO & LEO

Digital transformation has deeply affected all areas of society, including industry and economy, as well as governmental domains, such as defence and security.

Security organisations and armed forces have structured a new business model on modern, interoperable, scalable and service-oriented IT. Its core and support processes are Command, Control, Communications, Computers, and Intelligence (C4I). These serve as an indispensable basis for Network Enabled Operations (NEO), networking relevant actors, units and facilities, as well as linking sensors and effectors together. C4I delivers situational awareness when and where it's needed to support decision-making. This real-time situational awareness vastly increases the agility of forces to manoeuvre and respond.

Space based information and communication services deliver earth observation, position, navigation and timing, space situational awareness and communication. This enables high mobility and precision; quick deployment and wide geographical coverage; and independence of terrestrial infrastructure; secure high bandwidth and ubiquitous coverage; highly scalable content distribution; connecting fixed and on-the-move 5G network sites. Consequently, space capabilities have become central to NEO, including missile warning, geolocation and navigation, target identification, and tracking of adversary activities.

Military Command and Control will use space-based system coupled with meshed networks systems to support deployed operations and allow data exchange in austere environments wherein units will join ad hoc networks built upon the devices belonging to the friendly forces. Mobile communication devices will share intelligence, translate languages, provide navigation, targeting data and blue force position while maintaining visual contact with the surrounding environment. This will prove particular valuable in hybrid warfare, as terrestrial communication infrastructure may not be accessible.

Built on lessons learned from the Afghanistan the development of the Federated Mission Networking (FMN) has been among the most valuable new capabilities of the past decades that has remarkable potential for the developing space environment. FMN is a capability aiming to support command, control and decision-making in future operations through improved information-sharing. It provides the needed agility, flexibility and scalability in challenging mission environments. It´s based on principles that include cost effectiveness and maximum reuse of existing standards and capabilities.

Operational Concepts dealing with FMN assume that some or all military actors are sharing information within a FMN environment. FMN provides instructions for rapidly forming a federation of multinational military networks, leveraging agreed standards and protocols to create a common information environment. FMN also

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

offers capabilities that will be required to share information between FMN participants and non-FMN entities, including Non-Governmental Organizations (NGOs), International Organizations (IOs) and private sector organizations.

As unmanned platforms, cyber systems and human-machine teaming become prevalent, the effectiveness of operational units will be determined by how quickly information can be processed and transmitted. On the future battlefield, every soldier, satellite, and vehicle should be digitally linked. Uniform and ubiquitous communications is a "critical enabler" for a joint, networked multi-domain hybrid warfare environment.

Consequently, federated approaches should also guide satellite architectures and processes thus providing for networks of spacecraft trading previously inefficiently allocated and unused resources such as downlink bandwidth, storage, processing power, and instrument time. This holds the promise to enhance cost-effectiveness, performance and reliability of existing and future space missions, by networking different missions and effectively creating a pool of resources to exchange between participants in the federation to include ground-, air- and sea-based communication systems. Such a concept would also be beneficial to satellite operators, space agencies, and other stakeholders of the space industry as it drastically increases the flexibility to interoperate space systems as a portfolio of assets, allowing unprecedented collaboration among heterogeneous types of missions.

On the industrial side the digitalisation of industry and economy drive growth. As such, the space industry benefits from advanced capabilities, business models and services. Industry 4.0 is revolutionising collaboration, production and services, as well as the fundamentals of successful competition. It provides the emerging environment in which computers and automation come together in a new way with remotely connected robotics, guided by computers equipped with AI. This allows for the learning of algorithms, which permits robotics control and adaptation with very limited human interface.

Hardly a day goes by without an innovative space related technology. Satellite communications have fuelled the majority of commercial growth since the 1980s. GEO satcom operators have developed wholly new satellite designs, fleet architectures, and ways of engaging with customers that enable greater system-level flexibility and responsiveness. Digital-enabled satellites for medium and low earth orbit (MEO and LEO) are key parts of this transformation, and a significant upgrade from geostationary orbit satellites (GEO); the combination of LEO, MEO and GEO capabilities provides for significant synergetic capacities.

The defence and security community has recognised the powerful capabilities of these emerging constellations in enabling NEO. The closer proximity of LEOs and MEOs to Earth allows them to deliver ultra-high bandwidth with much less delay as compared to Geostationary Orbit (GEO) satellites. MEOs and LEOs support real-time command-and-control applications, including transporting Unmanned Aerial Vehicle (UAV) Intelligence, Surveillance and Reconnaissance (ISR) data from an area of operation to analysis centres in respective headquarters anywhere in the world. Secure embassy communications, police, intelligence and special forces requirements are other perfect fits. The SES-owned MEO is already performing in orbit, thus bringing new capabilities to a variety of users. Others will follow.

In particular small satellites have triggered the interest of the communication-based service sector. They could, for instance, be of use with regard to the Internet of Things, machine-to-machine data exchange using the automatic identification system and when tracking aircraft in flight. SpaceX is just one of many companies eager to launch large constellations of satellites into space, in order to offer global internet coverage.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Companies like One Web, Telesat, LeoSat, and Amazon are also working on massive constellations that would provide internet connectivity from low orbits over Earth.

3. Actors & Vectors

Cybersecurity threats to space infrastructure are a relatively new phenomenon. For a long time, space used to be an ecosystem of its own. As longstanding technological and cost barriers to space have fallen, more countries and commercial firms have begun participating in satellite construction, space launch, space exploration etc. Along with these developments, both new opportunities and new risks for space-enabled services have emerged. Today, with the sophisticated knowledge garnered from satellite command & control and data distribution networks, it is increasingly understood that space assets have been far too vulnerable to cyber-attack. Actors can use offensive cyberspace capabilities to enable a range of reversible to no reversible effects against space systems.

Cyber threats manifest themselves against Space systems through:

- Jamming, Spoofing
- Ground infrastructure supporting control, telemetry systems, launch and mission control
- Deployed outer space satellite infrastructure
- Kinetic and Directed Energy capabilities
- Evolving protocols
- Transfer across IP networks
- Corporate supply chain
- International challenges
- Etc.

Florence Parly, French Minister of the Armed Forces, highlighted recently: *"Cyber capabilities have become … (an) … important asset to impact on … spacecraft or their control centres and ground stations and interrupt their service and functionality."*[2] Unfortunately, cyber threats are very hard to detect, and even when discovered, it is difficult to pinpoint and hold responsible the actors behind such attacks.

Cyber threats stem from a crowded scene of both foes and friends, criminals and terrorists, individual hackers and hacker groups, self-inflicted and insider threats. The threat may come from a developer who has accidentally, or otherwise, introduced malware into a system or an item of equipment, or from the integrator. It may come from the maintenance supervisor or the user, propagating malware via tools or simply by connecting a standard medium, such as a USB stick. It may also take the form of an intentional external attack.

China has supported cyberespionage against U.S. and European satellite and aerospace industries for over a decade.[3] It has been targeting network-based C4I, logistics, and commercial activities. It also plays a role in cyberespionage targeting foreign space entities, industrial and technical intellectual properties. There is a legacy of Russian cyber-attacks. For example, in 2015, a Russian group of hackers with connections to Russian

[2] Florence Parly. French Minister of the Armed Forces. Remarks on Space & Defence at the French space agency's Toulouse headquarters. September 7th, 2018. Posted in English translation on 23 September 2018 by gosnold https://satelliteobservation.net/2018/09/23/space-defence-policy-speech-by-the-french-ministry-of-the-armed-forces/…
[3] DIA. Challenges to Security in Space. January 2019. http://www.andrewerickson.com/wp-content/uploads/2019/02/DIA_Space-Security-Challenges_201901.pdf

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

intelligence hijacked unencrypted commercial satellite connections in order to steal data. Similarly, North Korea and Iran have advanced cyber capabilities, along with a history of attacking international assets in the cyber domain.

Satellites have a variety of access points which can be exploited by cyber-attacks – including the antennae on the satellites, the ground stations, and the earth-based user terminals. Attacks can range from stealing data, to sending fake or corrupt data, to a complete shutdown of all the satellite's operations. Cyber-attacks aim in particular at gaining unauthorised access to the satellite's instruments, bus, and data. Malware is a common vector for these attacks; it is introduced into hardware in the supply chain, and thereby compromises the ground units that communicate with satellites, including the ground control stations of the Satellite Control Network or field-deployed SATCOM radios.

Primary attack vectors aim at vulnerabilities in mobile and stationary ground segment components through which an attacker can compromise the confidentiality, integrity, or availability of a satellite. Because satellites must accept communications, including command and control information from the ground segment, compromising the ground segment may enable an attacker to take control of a satellite completely. This threat is particularly potent if there is a single bus for all types of telemetry received by the satellite, as this enables an attacker to use this path to send steering commands to the satellite.

A further aspect, ground systems have many of the same software vulnerabilities that plague other computer systems. But these vulnerabilities may be particularly prevalent in the space sector. This is because the majority of the satellites and ground stations on which modern technology depends are in fact decades-old, and frequently use highly vulnerable, legacy software and protocols. This is of particular concern, as the space segment of space systems was believed to be beyond access by malicious actors, with outer space serving as a kind of fence. As a result of this thinking, most security in the space segment relies on a secure ground segment. However, if the ground segment should be breached, the space segment is virtually unprotected. There is no fence in outer space. Consequently, a hacker that succeeded in compromising the ground-control station, could take complete control of a spacecraft. The attacker could also leave behind an advanced persistent threat (APT) – a stealthy set of hacking processes that continuously affect a system over time, to make strategic use of compromised satellites at later times.

Against this backdrop, cyber situational awareness has to deliver inputs based on a common sharable cyber operational picture. A designated common cyber operational picture needs to synthesise the current performance of cyber systems and operations, as well as current threats into an integrated picture. It reports status, vulnerability, threats, suspicious activity, and mission impact. It provides real-time information to tactical, operational and strategic decision-makers.[4]

4. Cybersecurity Beyond Earth

Innovation in space technologies has increasingly been driven by security and defence needs. Consequently, the tasks of securing outer space and cyberspace are converging. There is a premium on disruptive and game-changing technologies that are autonomous, reconfigurable, agile and adaptable. These include:

- Real-time, multi-domain space situational awareness;

[4] U.S. Fleet Cyber Command/Tenth Fleet, *Strategic Plan 2015-2020*. pg. 18, http://www.navy.mil/strategic/FCC-C10F%20Strategic%20Plan%202015-2020.pdf (Accessed: 06-11-2018)

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

- Predictive and automated threat analysis;
- Automated cyber forensics;
- Autonomous and automated space systems;
- On-board resilient and self-healing satellites to withstand shock and stress from natural or manmade events;
- New technologies in space ground operations, i.e. enhanced predictive technologies, dynamic encryption, and signal beaming based on mission needs or threats.
- Improved visualisation;
- Artificial intelligence and cognitive electronic warfare systems that augment human decision-making;
- Technologies to advance Quantum capabilities in the areas of computing and cryptography.

Yet, the commercialisation of space heightens cybersecurity concerns. Market incentives to lower costs and innovate quickly often come at the expense of software and hardware security. As space assets become simultaneously more connected and more vulnerable than ever before, the industry will need to push hard to address cybersecurity concerns.

The good news is: the European Union is getting ready to support disruptive technologies. With the proposals of the EU Space Programme and the European Defence Fund, it has provided a foundation to accelerate change. Both programmes link with other initiatives of the European Commission, for instance on critical infrastructures and technologies, cybersecurity, and quantum technologies – where China already has an edge.

Governmental Satellite Communications (GOVSATCOM) is another key space initiative of the EU at the crossroads of space, security and defence. GOVSATCOM's objective is to ensure reliable, secure and cost-effective satellite communication services in both the civil and military environment. These services are then used by the EU and by national public authorities managing security-critical missions and operations. The idea being, thus, to make use of affordable and innovative solutions in synergy with industrial players. Here, LuxGovSat, a public-private joint venture between the Luxembourg government and SES, has moved into a comfortable position. Targeting exactly this emerging market, the company launched its first satellite, called GovSat-1, on January 31, 2018. It uses government-use frequency bands, i.e. X-band and military Ka-band. This enables a broad spectrum of applications, thereby delivering connectivity to theatres of operation, institutional and defence sites.

Transferring the upcoming hybrid and disruptive technological challenges into a viable, security/defence capability that also pays off on European and global markets is the core of the upcoming cybersecurity challenge. Improving space cybersecurity requires extending good cybersecurity practices into the commercial space sector and addressing problems specific to space activities. Advice for this sector repeats familiar mantras, such as the need for intra-sector and international collaboration, information sharing, enterprise risk management, encryption, insider threat prevention, and supply chain protection. AI and Quantum technologies will have an important role. Inadequate international legal regimes need to be addressed. NATO, EU and member nations security policies need to come up with appropriate guidance.

To get there, an innovative ecosystem is needed fostering novel approaches by key operators. While there is already significant change in the space industry, there is still much more to come. The role of industrial IT suppliers needs to be considered carefully – good examples of what we are seeing with innovation and new

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

technologies in the US have been borne out of closer collaboration with industry – sharing technologies, working differently in hubs etc. There are many best practices – where a new 'more progressive partnership model' that blurs boundaries is yielding results.

Capability and future workforce planning are critical. Traditional military planning techniques may not identify the workforce inputs and partnerships required to adopt in line with the rate of change. Technologies are evolving fast. Consequently, innovative, courageous, highly capable engineers, specialists and professionals must be developed. Co-ordination is also critical. Many different parts of organisations are trialling / investigating / building capabilities – however they are often drawing on the same scarce skill sets and industry capability.

The stage has been set for a rapidly expanding and highly interactive space-based economy moving forward, with cyber as a key driver. The technological advancement — from within the industry and beyond — demands the sector's constant evolution. New players are finding opportunities to deploy communications systems which diverge from the pre-existing models of their competitors. Taken as a whole, this drives the emergence of new markets and space-based business models. Governments, commercial customers and industry should all prepare themselves for new business models and the new economics of space as there is substantial change coming up. Cyber is the driver.

***

Remarks: The opinions expressed in this contribution are those of the author.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Author of this Issue

Ralph D. Thiele, born in 1953, is President of EuroDefense, Germany, Managing Director StratByrd Consulting, Germany, Chairman Political-Military Society, Germany and Member Advisory Board German Employers Association, Wiesbaden. He is a retired Colonel, held in his 40-year military career in the German Armed Forces key national and international positions. He

- Commanded troops up to the battalion level;
- Developed concepts and capability requirements in the Ministry of Defence;
- Drafted speeches and policy papers for Federal Presidents, Ministers of Defence, Major NATO Commanders and Service Chiefs;
- Drove educational innovation at the German Armed Forces Command and Staff College (Director Faculty) and at the NATO Defense College (Chief of Staff);
- Shaped the Bundeswehr's path towards network enabled capabilities (Commander Bundeswehr Transformation Command).

In his honorary and business functions he advices on Defence Innovation and Cyber issues in times of digital transformation. He has been frequently consulting, publishing and lecturing in Europe, America and Asia.

Ralph D. Thiele is also a member of the ISPSW Speaker Management Team. Further information at ISPSW website: http://www.ispsw.com/en/speaker-management/


Ralph D. Thiele

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de