UNIVERSITÄT OSNABRÜCK
LV Geopolitics and Geostrategy
Department 1
49069 Osnabrueck

Advances in Electronic Warfare

28 Oct 2021

Summary
Electronic warfare (EW) is any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. During Cold War, electronic warfare was an important military activity; a typical attack method was jamming (disturbance) of communication frequencies and radar signals. After cold war, the focus shifted to network-centric and cyber warfare and drove attention away from traditional EW.
Meanwhile, the development of directed energy (laser and high-powered microwave) weapons has made substantial progress. In particular, the US and Chinese Navy have advanced prototypes of military laser weapons and first reports of real-world attacks exist. In the United States, electronic warfare and cyber warfare are now integrated in the concept of cyber electromagnetic attacks (CEMA).
Moreover, satellites and their communication lines are increasingly important, but they are vulnerable for CEMA. The concept of space resilience was developed as a technical backbone of space defense. This working paper provides a brief overview and background on EW and CEMA, followed by an overview on directed energy weapons and security issues with a particular focus on laser weapons and satellites.

Contents

1. Fundamentals

1.1 Overview

The electromagnetic spectrum is the range of frequencies of electromagnetic radiation from zero to infinity. The lower the frequency, the lower the energy and the longer the wavelength[1].

All parts of the spectrum can be utilized for military purposes[2]. The military uses very low frequency radio waves to communicate with submarines underwater, radio frequencies to communicate with friendly forces; microwaves as data-links, radars, and satellite communications including situational awareness by radar and light detection and ranging (LIDAR) systems; infrared for intelligence and to target enemies; and lasers in the infrared and ultraviolet ends to communicate, transmit data, to dazzle intelligence collection sensors and potentially destroy a target[3]. Missiles in general, and anti-air munitions in particular, use either infrared or radar for terminal guidance to targets[4]. X-rays are routinely used for aircraft maintenance to identify cracks in airframes. Finally, gamma rays are high-energy radiation and help identify potential nuclear events[5]. The following table provides a brief overview.

Table 1 The Electromagnetic Spectrum [6]

Group	Subgroup	Comments
	Extremely low frequency ELF	Geomagnetic sources
Radio spectrum	Very low frequency VLF Low frequency LF Medium frequency MF High frequency HF Very high frequency VHF Super high frequency SHF Extremely high frequency EHF	The radio frequency spectrum covers radio broadcast, television and cell phones The EHF spectrum covers microwaves, which are also used for satellites
Light	Infrared (IR) Visible light Ultraviolet (UV)	Emitted by sunlight
Radiation	x-rays gamma rays cosmic x-rays	Radiation is harmful by damaging human DNA

Source: US Army Field Manual FM 3-38, Figure 1-3

In the United States, **Electronic warfare (EW)** is defined as *"any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy"*[7]. Electronic warfare consists of the three divisions electronic attack, electronic protection, and electronic warfare support. Table 2 provides an overview[8].

[1] Field Manual 3-38, Section 1
[2] Hoehn 2021a, p.1
[3] Hoehn 2021a and 2021b
[4] Hoehn 2021a, p.3
[5] Hoehn 2021a, p.1
[6] Field Manual 3-38, Figure 1-3
[7] Field Manual 3-36, Section 1
[8] Field Manual 3-36, Section 1-17

Table 2 The Electronic Warfare Divisions

Divisions	Purpose	Activities
Electronic attack	The use of electromagnetic energy, directed energy, or antiradiation weapons	**Countermeasures** (electro-optical-infrared and radio frequency countermeasures to block precision guided weapons and sensor systems)
		Electromagnetic deception (to convey misleading information to enemy)
		Electromagnetic intrusion (intentional insertion of electromagnetic energy into transmission paths to deceive operators or to cause confusion)
		Electromagnetic jamming (deliberate radiation, reradiation, or reflection of electromagnetic energy)
		Electromagnetic pulse EMP (radiation to produce damaging current and voltage surges). An EMP could be caused by nuclear weapons, but may also naturally occur as an effect of strong solar storms[9].
		Electronic probing (intentional radiation for learning the functions and operational capabilities of the devices or systems)
Electronic protection	Actions taken to protect personnel, facilities, and equipment	**Electromagnetic hardening** (protection against undesirable effects of electromagnetic energy)
		Electronic masking (controlled radiation of electromagnetic energy on friendly frequencies)
		Emission control (selective and controlled use of electromagnetic, acoustic, or other emitters)
		Electromagnetic spectrum management (planning, coordinating, and managing joint use of the electromagnetic spectrum)
		Wartime reserve modes (deliberately held in reserve for wartime or emergency use)
		Electromagnetic compatibility (ability of systems to use electromagnetic spectrum without degradation or interference)
Electronic support	Actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy.	**Electronic reconnaissance** (detection, location, identification, and evaluation of foreign electromagnetic radiations)
		Electronic intelligence (technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations other than nuclear detonations or radioactive sources)
		Electronics security (all measures designed to deny unauthorized persons information of value)

Source: US Army Field Manual FM-36-3, Section 1 (abbreviated wording)

Signals intelligence (SigInt) is intelligence information derived from signals and includes communication intelligence (COMINT), electronic intelligence (ELINT) and foreign instrumentation signals intelligence (FSINT). Signals intelligence systems primarily collect spectrum emissions passively, i.e., they do not emit their own signal. The SigInt is covered by the *National Security Agency (NSA)*. The difference between SigInt and EW support is that the EW support is tactical, i.e., only limited to the needs for a certain situation at a certain timepoint, but EW support and signals intelligence missions use the

[9] Morschhäuser 2014, p.1-2

same resources[10]. Signals intelligence above the tactical level is under the operational control of the NSA.

The **Spectrum Operations** include the

- **signature management** where weapons systems reduce their electromagnetic signature to reduce the probability of detection, interception and destruction;
- **Navigation Warfare (NAVWAR)** as *"deliberate offensive and defensive actions to assure friendly use and prevent adversary use of positioning, navigation, and timing information through coordinated employment of space, cyberspace, and electronic warfare capabilities. NAVWAR is further enabled by supporting activities such as* ***Intelligence, Surveillance, and Reconnaissance (ISR)*** *and* ***electromagnetic spectrum (EMS) management"***[11].
- Also, Command and Control (C2) systems are supported.

1.2 History of Electronic Warfare

Jamming of communication signals was then already done to a limited extent in 1904 in the Russia-Japanese war and in World War 1. In World War 2, radar systems and radar jamming emerged as new phenomenon. Further advances in tactics and technology occurred during the Vietnam War in air tactics[12].
During Operation *Enduring Freedom* in Afghanistan and Operation *Iraqi Freedom* in Iraq, the U.S. Army used new electronic attack (EA) capabilities to jam radio-activated triggers and defend friendly forces against radio-controlled improvised explosive devices [13].

After the end of Cold War, the dominance of the US enabled the uninterrupted use of the *Global Positioning System (GPS)* with unhindered communications. As a result, concepts such as radio discipline, electromagnetic signature control, and frequency hopping became less important[14]. Also, the cyber warfare emerged and drove attention away from traditional EW. But meanwhile, Russia and China have significantly upgraded their EW capabilities. In Eastern Ukraine, Russian-backed forces used sophisticated jamming and interception tactics to undermine communications and surveillance drones[15]. The development of directed energy weapons and the expansion of EW capacities to outer space by satellites are further reasons for the rapid re-emergence of electronic warfare.

1.3. Cyber Electromagnetic Attacks (CEMA)

1.3.1 Definition and Concept

In 2014, the United States integrated cyber warfare and electronic warfare into the new concept of **cyber electromagnetic activities (CEMA)**. The *US Army Field Manual 3-38* defines: *"Cyber electromagnetic activities are activities leveraged to seize, retain, and*

[10] Field Manual 3-36, Section 1-17
[11] DoD cited by Hoehn/Sayler/Gallagher 2021
[12] von Spreckelsen 2018, p.42
[13] APT 3-12.3 2019, Section 1-3
[14] von Spreckelsen 2018, p.42
[15] von Spreckelsen 2018, p.42

exploit an advantage over adversaries and enemies in both cyberspace and the electromagnetic spectrum, while simultaneously denying and degrading adversary and enemy use of the same and protecting the mission command system"[16].

While cyber capabilities area used to achieve objectives in and through cyberspace, electromagnetic and directed energy are used to control the electromagnetic spectrum or to attack the enemy[17]. Obviously, electromagnetism plays an important role for the cyberspace as well. There is the power supply by electric energy, while bits (0 and 1) are certain magnetic conditions on storage media. The electronic warfare targets the electromagnetism, i.e., the physical component of the cyberspace.

The **information environment** is defined as *"the aggregate of individuals, organizations, and systems that collect, process, disseminate, or act on Information"* [18] with three dimensions, physical, informational and cognitive. While the electromagnetic component resides within the physical dimension, the three layers of cyberspace (physical, logical, and cyber persona) reside within the physical and informational dimensions of the information environment[19].

Note that the electromagnetic spectrum management appears in the definition of electronic warfare and then in a similar way in the CEMA concept as **Spectrum Management Operations (SMO).** The difference is that within CEMA this activity is part of a broader concept. Spectrum Management Operations (SMO) include *"the spectrum management, frequency assignment, host-nation coordination, and policy that enable the planning, management, and execution of operations within the electromagnetic operational environment during all phases of military operations"*[20].

In summary, CEMA are implemented via the integration and synchronization of cyberspace operations, electronic warfare (EW), and spectrum management operations (SMO) [21].

On a higher level, United States perform **inform and influence activities (IIA)** *"to affect the information environment in order to synchronize themes, messages, and actions with operations to inform United States and global audiences, influence foreign audiences, and affect adversary and enemy decision-making"*[22]. Within this broad approach, cyber electromagnetic activities are considered information-related and must be integrated and synchronized with other information-related capabilities.

[16] Field Manual 3-38, Section 1-1
[17] Field Manual 3-36, Table E-1
[18] Field Manual 3-38, Section 1-18
[19] Field Manual 3-38, Section 1-18
[20] Field Manual 3-38, Section 1-7
[21] Field Manual 3-38, Introduction
[22] Field Manual 3-38, Section 1-23

Table 3 Cyber electromagnetic attacks (CEMA)

Division	Purpose	Activities
Electronic Warfare	Electronic attack	The use of electromagnetic energy, directed energy, or antiradiation weapons
	Electronic protection	Actions taken to protect personnel, facilities, and equipment
	Electronic support	Actions to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated electromagnetic energy.
Cyberspace Operations	Cyber situational awareness	The knowledge of relevant information regarding activities in and through cyberspace and the electromagnetic spectrum
	Network operations	Activities conducted to operate and defend the Global Information Grid*
	Cyber warfare	Warfare that extends cyber power beyond the defensive boundaries of the Global information Grid to deny, degrade, disrupt, destroy, and exploit enemies.
Spectrum Management Operations (SMO)	To coordinate and to de-conflict frequencies to enable systems to perform their functions without causing or suffering unacceptable electromagnetic interference[23]	spectrum management, frequency assignment, host-nation coordination, and policy for spectrum dependent devices, including air defense radars, navigation, sensors, munitions using the electromagnetic spectrum, manned and unmanned systems of all types (ground and air, radar, sensor).

Source: US Army Field Manual FM 36-3, Appendix E and FM 38-3, Section 5
*Note: Global Information Grid is the term for the US military computer network, but for other countries this could be generalized to "military computer network"

Moving on, the focus of this working paper will remain on the EW part, for a full presentation of cyber warfare please refer to the open access working paper 2019 Cyberwar-methods-and-practice
https://repositorium.ub.uni-osnabrueck.de/handle/urn:nbn:de:gbv:700-201907091696
and its 2020 update under
https://repositorium.ub.uni-osnabrueck.de/handle/urn:nbn:de:gbv:700-202009303605.

1.3.2 Practical Implications

In Sep 2021, the U.S. Army's first integrated Electronic Warfare, Cyber and Signals Intelligence platform which can be used on Stryker vehicles reached the advanced testing stage. The system is named *Terrestrial Layer System-Brigade Combat Team (TLS-BCT)* and is produced by *Lockheed Martin*. The idea behind is that soldiers can e.g., detect and visualize any electronic warfare threat on the battlefield[24].

[23] Field Manual 3-38, Section 5
[24] C4ISRnet.com 27 Sep 2021

1.4 EW Programs and Capabilities

Electronic Warfare (EW) capabilities can be divided terrestrial and airborne (which now also includes the space with satellites, refer to Section 3). **Terrestrial EW** sensors and jammers on land or on ships are limited by the available power and the local situation, they are focused on intercepting and jamming radios and artillery radars. **Airborne EW** is used to intercept, decrypt, and disrupt communications, radars, and other command and control (C2) systems over a large area.

1.4.1 United States

All parts of the US military are undergoing modernization efforts to achieve Electromagnetic Spectrum Superiority.

Terrestrial electronic warfare programs can be grouped as follows:[25]

- **Counter-improvised explosive device (C-IED)** systems jam IED communications radio frequencies to prevent them from detonating. These frequencies include cell phones, small two-way radios, and other basic radio communications.
- **Counter-unmanned aerial systems (C-UAS)**, or simply counter-drone systems can detect and/or attack drones. In 2019, 235 counter-UAS products were counted. The Army has recently tested a 5-kilowatt (kW) laser, which is placed on a Stryker-armored vehicle and can destroy small drones, but a problem is the need for a power supply which is still (too) large for operational practice.
- **Communications and radar jammers**: The Army's primary communications jammer is the *EW tactical vehicle (EWTV)*, a vehicle to sense and to jam enemy communications. Further advanced systems are in development[26].

Electronic warfare aircrafts detect and jam enemy radars and air defense command-and-control equipment; the US has three primary manned EW electronic attack aircraft types. The new *F-35 Joint Strike Fighter* has an electronic warfare system called AN/ASQ-239 for signal collection, radar warning, geolocation of electronic emitters, tracking of multiple aircrafts simultaneously and has a highly focused radio antenna for countermeasures and attacks[27]. A new jamming system for airplanes, the *Next Generation Jammer (NGJ)* is currently developed[28].

1.4.2 Russia and China

China and Russia have developed *anti-access/area denial (A2/AD) systems* to deny access to their communication and command and control. After the short war with Georgia in 2008, the experience was used for the *New Look Program* which resulted both in technical and organizational modernization[29]. The signals intelligence forces and EW forces are closely related. The idea is to block the enemies espionage (C4ISR) activities and to use

[25] Hoehn 2019a
[26] Hoehn 2019a
[27] Hoehn 2019b
[28] Hoehn 2019b
[29] Hoehn 2019a

EW for military operations. Russia reportedly has employed EW as part of its military operations in Ukraine and Syria[30].

China developed the concept of "**informationized warfare**," and organizes EW functions in a new command called the *Strategic Support Force*, which includes cyber, psychological, information, and space forces. The investments include ground-based and airborne sensors and jammers as well as space-based intelligence devices[31].

The close relation between cyber activities, information space and electronic warfare was also reflected by the reform of the *German Federal Army (Bundeswehr),* where since 01 April 2017 all activities in the cyber and information space[32] are led by the *Cyber and Information Space Command (Cyberinformationsraumkommando CIR)* with the units

- *German Army Secret Service for Exterior Affairs (Kommando Strategische Aufklärung KSA)* which is responsible for cyber network operations (CNO), analysis (Auswertung) and 4 battalions for electronic warfare (*elektronische Kampfführung EloKA*) [33]
- the *IT Command (Kommando IT Bundeswehr KdoItBW)* which covers software and security aspects and
- the military satellite unit (with the whole *Geoinformation GeoBw*).

2. Directed Energy Weapons

2.1 Introduction

Directed Energy weapons include **high-energy lasers (HEL), high-powered microwave (HPM)** and **particle beam weapons**[34]. Particle beams are already used in medicine for radiotherapeutic treatment of severe cancer since decades, but no weapons are ready for action yet.

2.2 High-Energy Lasers

2.2.1 Overview

Lasers have advantages and disadvantages[35]:

- As long as the laser has power, the laser can fire endlessly ('deep magazine') resulting in a low cost per shot ratio.
- The laser beam, if located in the infrared or ultraviolet spectrum, is invisible.
- It can be delivered with light speed and with high precision and potentially infinite range[36].

[30] Hoehn 2019a
[31] Hoehn 2019a
[32] Leithäuser 2015, p.4
[33] Der Reibert 2020, p.B-131
[34] Sayler 2021
[35] Hoehn 2021c, Sayler et al 2021
[36] Magnuson 2021, Eckel 2019

- Lasers however need to meet **size, weight, and power (SWaP)** and cooling requirements.
- Atmospheric conditions (e.g., rain, fog, obscurants) may lead to beam diffraction, spread, and absorption or scattering[37]. Technical adaptations may reduce this problem, but it cannot be completely avoided.
- A laser that continues firing in the same exact direction can heat up the air it is passing through, which in turn can defocus the laser beam, an effect called **thermal blooming**[38].
- Lasers can be less effective against targets that incorporate shielding, ablative material, or highly reflective surfaces, or that tumble or rotate rapidly[39].
- Some systems are small enough to fit on military vehicles, but many require larger and/or fixed platforms.
- There concerns how long such as system could survive in combat and limitations by **saturation attacks** (e.g., drone swarms which make it impossible to target them all), but these problems exist for conventional weapons as well.

High-energy lasers (HEL) were taken into consideration since the 1960ies, but the overall development takes much more time than initially expected[40].
Technically, there are different types of laser weapons[41]: **Solid-State Lasers (SSLs)** use a solid lasing medium, such as a rod made up of glass or crystal, or a gem, the *Neodymium Yttrium-aluminum* garnet (Nd:YAG) is widely used. A chemical laser uses chemical reaction to create population inversion in the lasing medium, while gas lasers use a pure gas or gas mixture to produce a beam.
Fiber Lasers are SSLs powered by electricity, and use optical fibers as the gain media. In 1973, TRW Inc. produced the world's first high-energy chemical laser, the Baseline Demonstration Laser, for the US Department of Defense[42].

The *Protocol on Blinding Laser Weapons, Protocol IV of the 1980 Convention on Certain Conventional Weapons of the United Nations* came into force on 30 July 1998 and prohibits to employ laser weapons specifically designed, as their sole combat function or as one of their combat functions, to cause permanent blindness[43].

All currently existing laser weapons are still more or less advanced demonstrators (prototypes), but at least the lasers of the US and Chinese navy ships could already be used for military practice. The focus of directed energy weapons on Navy ships is not surprising as the size, weight and energy needs of lasers make other applications difficult, a perspective that is shared by China as well[44].

[37] Sayler 2021
[38] Sayler et al. 2021
[39] Sayler et al. 2021
[40] Pugo/Galuga 2017
[41] Olson 2012
[42] Olson 2012
[43] Feickert 2018
[44] Peck 2021

A key problem of the laser weapon development is the requirement of mobility (on ships, armed vehicles, airborne). But is this restriction really necessary? A huge ground-based laser or a coordinated group of lasers on a mountain plateau (clean atmosphere) would be able to cover a large air and outer space sector and would be able to target satellites, missiles and hypersonic weapons.

2.2.2 United States

The U.S. military has a long history in developing directed energy (DE) Weapons, but now first practical results are seen.

HELs might be used in *short-range air defense (SHORAD), counter-unmanned aircraft systems (C-UAS), counter-rocket, artillery, and mortar (C-RAM) missions* or to "dazzle" (i.e., temporarily disable) or damage satellites and sensors[45].
While only a few kilowatts (kW) power are needed to affect small drones, it is assumed that laser with 100 kW could affect larger unmanned aircraft systems, small boats, rockets, artillery, and mortars. The US DoD plans to kilowatts increase power levels from currently around 150 kilowatts to around 300 kW in 2022, 500 kW in 2024, and 1 megawatt (MW) by FY2030. A megawatt laser could be able to destroy missiles and hypersonic weapons[46].

In August 2014, the US Navy has deployed their first *Laser Weapon System (LaWs)* on the USS Ponce to test functionality of laser weapons under maritime conditions, the first ever *US Department of Defense* laser weapon to be deployed and approved for operational use[47].
Furthermore, the 150 kW *Solid State Laser Technology Maturation SSL-TM* is installed on the USS Portland (LPD-27) [48].

By the end of 2021, the US Navy will set up the high-energy laser weapon *Surface Navy Laser Weapon System Increment 1* or *High Energy Laser with Optical Dazzler and Surveillance (HELIOS)* with above 60 kW kinetic energy (with growth potential to 150 kW) which is able to downing drones and boats on an Arleigh Burke Flight IIA DDG-51 destroyer[49]. It also has dazzling functions and an Intelligence, Surveillance, and Reconnaissance (ISR) sensor system if not used for attacks[50]. The laser is scalable by combining multiple laser fibers.
The destroyer class IIA was chosen, because older classes do not provide sufficient power supply for the laser while the newer class III already has too much electronic devices to have enough power for an additional laser weapon[51].

[45] Hoehn 2021c, Sayler et al. 2021
[46] Sayler 2021
[47] Feickert 2018
[48] O'Rourke 2021
[49] O'Rourke 2021
[50] Mizokami 2019, Magnuson 2021
[51] Dean 2019

Furthermore, the *ODIN (Optical Dazzling INterdictor) laser system* will be applied on seven destroyers to dazzle sensor of adversaries' drones[52]. The *HELCAP (High Energy Laser Counter Anti-ship cruise missile Program)* is still in an early stage[53].

An airborne laser project called *Self-protect High Energy Laser Demonstrator (SHIeLD)* is in progress. Various laser systems for placement on army vehicles are tested at the moment (in early stages), such as the 50 KW *Multi-Mission High Energy Laser (MMHEL*) for Stryker combat vehicles and a *High Energy Laser Tactical Vehicle Demonstrator (HEL TVD)* with 100 kW for installation on trucks[54].

2.2.3 China

In 2018, China presented a Laser Weapon System on a *People's Liberation Army (PLA) Navy Ship Type 055* destroyer which looks very similar to the US Navy laser weapon system on the *USS Po*nce[55]. The US Navy assumes that this may have to do with the cyber espionage activities of the sophisticated *Advanced Persistent Threat (APT) Temp.Periscope* which systematically attacked universities, contractors and organizations involved in maritime research since years[56]. *Temp.Periscope* is also active in other high-tech areas such as satellites and hypersonic weapon research.
China has reportedly developed a 30-kilowatt road-mobile HEL, *LW-30*, designed to engage unmanned aircraft systems and precision-guided weapons. China is also working on an airborne laser system[57]. Japan assumes that China develops anti-satellite laser beam weapons[58]. China is also working on a hand-held laser for crowd control which may be able to affect skin and clothing[59].

2.2.4 Further Actors

Other Asia-Pacific countries active in the area of directed energy and hypersonic weapons are India, Japan, Australia and Pakistan[60].

Russia has deployed the *Peresvet* ground-based HEL with several mobile intercontinental ballistic missile units and it is assumed that this is able to dazzle satellites and provide point defense against unmanned aircraft systems[61].
Russia is reportedly developing a weapon that can disrupt *Global Positioning System (GPS)* navigation signals and destroy radio communications equipment and satellites.

[52] Dean 2019
[53] Dean 2019
[54] Feickert 2018
[55] The Maritime Executive 2019
[56] The Maritime Executive 2019
[57] Peck 2021
[58] Rajagopalan 2015
[59] Yeo et al. 2021
[60] Yeo et al. 2021
[61] Hoehn 2021c

Russia plans to mount lasers with greater attack capabilities on their sixth-generation aircraft, which are not likely to be operational until the late 2030s[62].

In Germany, the drone defense research is going forward to the use of laser weapons. In May 2015, a small quadrocopter drone could be destroyed after application of 20 Kilowatt over 3.4 seconds[63]. The German laser weapon program is a joint effort of German research institutes and German industry in cooperation with the *German Ministry of Defense*. In the last decade, the two German companies *Rheinmetall* and *MBDA* have been putting up various technology demonstrators up to 50 kW and the two companies intend to construct, integrate and test a laser demonstrator for the German Navy's corvette K130[64]. However, in 2021 the German government could not predict when laser weapons will be ready for military practice[65].

2.2.5 Real-World Laser Attacks

In May 2018, the United States reported that in Djibouti, where both the United States and China are present with military bases, China has repeatedly used lasers to interfere with US aircraft landing[66].
While it is meanwhile a common bad practice that laser pointers are misused by civil persons to blind pilots (or goalkeepers in football stadiums) temporarily, at least three times military-grade lasers were used in the above-described incidents and two pilots suffered from minor eye injuries[67]. In the same year, it was reported that US military aircrafts were attacked more than 20 times over the East Chinese Sea, also Australia in one case. On 17 Feb 2020, a US *P8-A Poseidon* surveillance aircraft was hit by a laser beam from a Chinese *Luyang III* class destroyer 380 miles west of Guam[68].

2.3 High-Powered Microwave (HPM) Weapons

Important aspects of HPM weapons are[69]:

- deep magazines (i.e., no need for a physical ammunition), low costs per shot, fast engagement times, and can produce graduated effects
- HPM can generate waves at different frequencies and power levels to temporarily or permanently disrupt selected electronic systems
- They can have broad effects and can be non-lethal.
- Theoretically, HPM weapons could potentially generate effects over wider areas than HELs, e.g., as area defense against missile salvos and swarms of drones[70].

[62] Feickert 2018
[63] Marsiske 2016
[64] Eckel 2019, p.1-2
[65] Bundesregierung 2021, point 16 and 17
[66] Cronin/Neuhard 2020
[67] Cronin/Neuhard 2020
[68] Cronin/Neuhard 2020
[69] Sayler et al. 2021
[70] Sayler 2021

- HPM beams are more diffuse than lasers and the energy per unit area decreases significantly over distance[71].
- The waves may inadvertently damage other friendly systems as well.
- Microwaves can be stopped by solid walls as countermeasure.

It was reported that an HPM weapon might be responsible for the *Havana Syndrome*, the term used for symptoms like headache, sickness and others experienced by U.S. Embassy personnel in Havana (Cuba), but meanwhile also in other countries. However, this could not be clarified so far and the investigation is still ongoing. [72]

A variety of HPM systems have been provided to Army units in Iraq and Afghanistan to counter *Improvised Explosive Devices (IEDs)* used to attack vehicle convoys and troops on foot[73]. The *Active Denial System (ADS)* was a nonlethal counter personnel weapon that projects a focused millimeter wave energy beam that induces a painful heating sensation on an adversary's skin with the intent of repelling individuals without injury. The system was deployed to Afghanistan, but not used to avoid the impression that "radiation" would be used[74]. In 2014, China reportedly introduced its *WB-1 microwave active-denial system*, similar to the US Active Denial System.

3. Satellites

3.1 Introduction

A satellite is an object that has been intentionally placed into orbit, in 2019 several thousand satellites are assumed to be in orbit, less than half of them approximately still operational. Around 2,000 active satellites are in orbit controlled by more than 100 governments as well as commercial entities from more than 50 countries[75]. However, tens of thousands of small satellites are projected to launch in this decade for communications and Earth observation[76]. Satellites can serve a lot of functions[77], in particular

- **Earth observation**: land monitoring, marine environment monitoring, atmosphere monitoring, climate change, emergency management and security
- **Space observation** including detection of near-earth objects such as asteroids
- **Global satellite navigation systems** for accurate and reliable positioning and timing information for autonomous and connected cars, railways, aviation and other sectors, in particular the *Global Positioning System (GPS)* from US, *Galileo* from Europe and *Glonass* from Russia. High-precision navigation is reserved for military purposes.

[71] Sayler et al.2021
[72] Sayler 2021
[73] Feickert 2014
[74] Feickert 2014
[75] CRS 2019
[76] Pekkanen 2019, p.93
[77] EU 2019

- **Communication Satellites** for television, data transfer and telecommunication in particular in regions where it is difficult to build infrastructure, because otherwise earth and deep-sea cables may have much higher data flow rates.
- **Espionage and Reconnaissance**: The information from satellite pictures is also known as **Imaging Intelligence (IMINT)**. The largest satellite-based intelligence organization is the United States *National Reconnaissance Office (NRO)*. Another satellite imaging organization is the *National Geospatial Agency (NGA)*. Satellites stepwise replaced spy planes which were initially used after World War 2. The EU has a Satellite Center *EU SatCen* which supports the *Intelligence Center IntCen*.
- **Military satellites** for detection of missile attacks or as 'killer satellites'.

3.2 The Strategic Role of Satellites

Satellites are of growing strategic relevance for three reasons:

- The first aim is to achieve a **better global coverage**. Note only the number of civil satellites (in particular the *Starlink* satellite network with thousands of new satellites in the 2020ies), but also the number of military and espionage satellites is rapidly growing.
- The second aim is to achieve a **better imaging quality and faster and more precise analysis**. Here, Artificial Intelligence plays a key role, in the US military the *Project Maven*.
- The third aim to give satellites a more active role in military operations by having a **closer relation between threat detection and response**, in the US military the *Joint All-Domain Command and Control project* and Project *Prometheus*[78].

But there also civilian projects like *Starlink* from *SpaceX* which will increase the number of satellites and would have significant impact on daily life, but also increase the vulnerability of societies against satellite attacks which shows the importance of satellite security[79].
In a study for the *RAND Corporation*, Weinbaum et al. found commercially available EW capabilities for eavesdropping, jamming, and hijacking of satellite communications[80].

3.2.1 Global Coverage

The leading nation working with any kind of satellites are the United States. A recent count estimated for the US 154 military satellites and 49 satellites of the satellite-based intelligence organization *National Reconnaissance Office (NRO)*. China had in the same count 63 and Russia 71 (known) satellites, while other countries had less than ten each.

[78] Strout 2021
[79] Hlavica 2019
[80] Weinbaum et al. 2017

The Intelligence, Surveillance, and Reconnaissance (ISR) satellites ('spy satellites') can for examples detect and record hundreds of thousands of cell phone calls simultaneously and produce highest-quality images of the earth[81].

3.2.2 Imaging Quality and Analysis

The summary of the 2018 US Department of Defense DoD AI strategy states that "*AI refers to the ability of machines to perform tasks that normally require human intelligence—for example, recognizing patterns, learning from experience, drawing conclusions, making predictions, or taking action— whether digitally or as the smart software behind autonomous physical systems*."[82]

AI is expected to be particularly useful in Intelligence, Surveillance, and Reconnaissance (ISR) due to the large data sets available for analysis as in the above-mentioned *Project Maven*. But Imaging Intelligence (IMINT) is more than target identification or face recognition, the *Defense Intelligence Agency (DIA)* and the *Central Intelligence Agency (CIA)* for example supervise adversary buildings with restricted access to analyze activities[83].

The *DoD Joint Artificial Intelligence Center (JAIC)* coordinates since 2019 the efforts to develop, mature, and transition artificial intelligence technologies into operational use. *Project Maven* is active since 2017 for automating intelligence processing with computer vision and machine learning algorithms for target identification from drone data. Other AI programs include developing algorithms for multilingual speech recognition and translation in noisy environments, geo-locating images without the associated metadata, fusing 2-D images to create 3-D models, and analysis tools to infer a building's function based on pattern-of-life analysis[84].

3.2.3 Threat Detection and Response

The DoD *Joint Artificial Intelligence Center (JAIC)* is working on projects that should transfer information on threats detected by satellites into immediate response recommendations for commanders.
The *Joint All-Domain Command and Control* project seeks to connect every sensor to every shooter and in demonstrations, this cut down response time from detection to firing from 20 minutes to 20 seconds.
A part of this is the *Project Prometheus* of the US Army, which automatically detects threats in satellite imagery and *Project Firestorm* which is focused on creating response recommendations to commanders[85].

---

[81] Abbany 2020
[82] DOD 2018, p.5
[83] Folmer/Margolin 2020
[84] Hoadley/Sayler 2019, p.9-10, DoD 2018, OSTP 2020, NSCAI 2020
[85] Strout 2021

3.3 Attacks on Satellites

3.3.1 Overview

The threats to satellites can be categorized into:

- Space weather
- Anti-satellite (ASAT) missiles[86]
- Co-orbital systems[87]
- Space debris
- Cyber-attacks (see Section 3.3.2)
- Electronic warfare: jamming (including Navigation Warfare), laser beams for sensor dazzling or destruction (see Section 3.3.3)

Space weather caused by solar variability is a potential threat to space systems, human space flight and ground- and space-based infrastructures upon which societies increasingly depend. Solar winds have a similar effect like an electromagnetic pulse and can damage sensitive electronic elements.

Established weapons are **anti-satellite (ASAT) missiles** which however cause a lot of space trash which brings all other space objects into danger[88]. For testing purposes, satellites in low earth orbit have been destroyed by ballistic missiles launched from earth by Russia, the United States, China and India. The testing of anti-satellite weapons by China in 2007 and recently by India in 2019 caused additional debris to the space environment[89].

Co-orbital systems are satellites placed on similar orbits and can intercept or interfere with other satellites through close orbital rendezvous operations[90]. In 2017, the Russian *Louch-Olympus* spy satellite came very close to the French-Italian *Athena-Fidus* military satellite and has meanwhile 'visited' eight satellites[91]. In January 2020, it was reported that the Russian satellite *Cosmos 2542* came close to the US satellite *USA 245*. The orbit of *USA 245* was then changed, but *Cosmos 2542* was able to follow. Later on, it released a sub-satellite, *Cosmos 2543*, to continue the observation of *USA 245*[92].

Space debris: The space activities in the past 60 years have created an estimated 23,000 pieces of uncontrolled debris that can disable or destroy a satellite[93]. However, space debris can also be used to cover **virtual satellites**. Virtual satellites consist of small parts in slightly different orbits which wireless cooperate and act like a regular satellite. Virtual satellites are an attractive approach for spy satellites, but also for military **sleeper satellites**[94].

[86] Finkbeiner 2021
[87] Rajagopalan 2019
[88] Finkbeiner 2021
[89] CRS 2019
[90] Rajagopalan 2019
[91] DW 2019
[92] Finkbeiner 2021
[93] CRS 2019
[94] Abbany 2020

3.3.2 Satellite Hacking

3.3.2.1 Direct Cyber Attacks

Another weapon is satellite hacking which can be done as direct attack on satellites or as attack on the ground station and or providers. Little is published, but one can say that direct takeover of satellites in space is cumbersome and has little effect, while hacking of space control centers on earth has led to a substantial increase of satellite hacking activities.

Satellite hacks of US satellites were already reported since a decade and China was suspected by the *US-China Economic and Security Review* Commission since a longer time already[95]. In 2011, a report of this Commission stated that two US satellites had been compromised in 2007 and 2008 through a ground station in Norway and in 2014, the *US National Oceanic and Atmospheric Administration confirmed* that one of its satellites had been hacked[96].

The *Waterbug group* (aka *Turla/Snake/Ouroburos/Venomous Bear/Krypton/Group88*) is the name for the actors who use the malware *Wipbot/Tavdig/Epic Turla, Uroburos/Turla/Snake/Carbon* and *agent.btz/Minit.* In one source code the term UrObUr()s was used, alternative writings to *Uroburos* are *Ouroburos* and *Uroboros*. Western intelligence attributes this APT to the Russian civil intelligence FSB. The group owns a malware family that could be backdated to 2005. The group is utilizing satellite-based internet links for action[97].
Simply spoken, a sender sends data to a satellite as uplink, the satellite then sends data back to one or more receivers as downlink. The *Waterbug/Turla* group hijacks *DVB-S (digital video broadcasting satellite)* links with their own satellite dish by inserting their own data packages into the downlink signal to control their botnet. This method allows to act highly anonymously as the signal seems to come from a legitimate sender[98].

3.3.2.2 Cyber Attacks on Ground Stations/Control Centers

While in the past people thought that future wars on earth would be decided in space, it seems now that future wars in space may still be decided on earth: the hacking of space control centers could be used for sabotage, i.e., by sending false commands to move satellites resulting in damage, collision or loss. This does not only affect satellites, but is also applicable for all kinds of space robotics in general. Cyber-attacks included:

- The German Space Center *Deutsches Luft- und Raumfahrtzentrum DLR* was hacked in April 2014, presumably for technology espionage[99].
- In 2015, the French Television *TV5Monde* was temporarily taken offline by the Russian cyber group *APT28 (Fancy Bears)*[100]. The server for the satellite signals

[95] Menn 2018
[96] Rajagopalan 2019
[97] Weedon 2015, p.72-73
[98] Paganini 2015
[99] Die Zeit online 2014
[100] FAZ online 2015, p.1

was attacked and as the maintenance of this server was done by another vendor, a longer signal downtime was achieved[101].

- According to reports from June 2019, the NASA *Jet Propulsion Laboratory JPL* was accessed by connecting a *Rapsberry Pi* device, which then allowed to steal data from Mars missions[102]. In 2018, also the *JPL Deep Space Network* as system of satellite dishes for communication with Nasa spacecrafts was infiltrated. In December 2018, two members of the Chinese cyber group *APT10* were indicted for intrusion of the JPL, but it was not stated whether this specific attack was meant.
- In addition to ground stations, suppliers and stakeholders are also a security risk[103]. In June 2018, *Symantec* reported successful breaches of satellite and defense companies by a new espionage hacking group *(Advanced Persistent Threat APT)* called *Thrip* which has been active since 2013. This APT may have overlaps with the APT40 (*Temp.Periscope/Temp.Jumper/Bronze Mohawk/Leviathan*). APT40 is active since 2013 and attacks preferably industries involved into military ship construction.

3.3.3 Electronic Warfare in Outer Space

It is nowadays no problem to produce high-precision long-range laser beams, but it is currently still difficult to produce sufficient kinetic energy to impact larger objects. In principle, laser beams can dazzle sensors, but also damage and destroy satellites.
Japan assumes that China develops anti-satellite laser beam weapons[104]. China possibly already has a limited capability to employ laser systems against satellite sensors and a ground-based laser weapon that can counter low-orbit space-based sensors[105].
France is also intensifying research on laser weapons to defend their satellites[106].

Due to the low received signal strength of satellite transmissions, satellites are also vulnerable by jamming by land-based transmitters, e.g., to disturb GPS navigation satellites. To prevent this, the *US Department of Defense* has developed the concept of **Navigation Warfare (NAVWAR)** as deliberate offensive and defensive actions which is further enabled by supporting activities such as Intelligence, Surveillance, and Reconnaissance (ISR) and electromagnetic spectrum (EMS) management[107].
In a study for the RAND Corporation, Weinbaum et al. found EW/SigInt capabilities available outside government usage (either legal or illegal), including applications for **eavesdropping, jamming, and hijacking of satellite communications**.[108] As an example, jamming of satellite-signals was frequently reported in the Middle East region. As a consequence, the Satellite provider *Eutelsat* integrated anti-jamming techniques in 2013 for its satellites[109].

[101] Wehner 2016, p.6
[102] Cimpanu 2019
[103] Hlavica 2019
[104] Rajagopalan 2015
[105] Hoehn 2021c
[106] DW 2019
[107] Hoehn/Sayler/Gallagher 2021
[108] Weinbaum et al. 2017
[109] Weinbaum et al. 2017

The US military has established satellite-based electronic warfare capabilities, including the *Space Based Infrared System (SBIRS) constellation* program, *electronic intelligence by satellite (ELISA)* electronic intelligence satellites; and space-based radar systems[110].

3.4 Space Resilience

Based on the increasing threats, there is need for a concept of **space resilience** as the technical backbone of space defense. There is no official NATO definition, but resilience (or resiliency) is commonly understood as robustness and survivability[111].

The **space defense** needs to cover the **space segment** with spacecrafts, the **ground segment** with control center, ground station and remote centers as well as the IT facilities and the launch facility, and finally the **user segment** with customer terminals (such as satellite TVs)[112].

In general, space resilience can be achieved by[113]

- **Disaggregation** - the allocation of different missions, functions or sensors across separate subsystems,
- **Distribution** - separate subsystems perform the same mission and collectively behave as a single system, e.g., the Global Positioning System (GPS)
- **Proliferation** – using multiple units of the same system to provide technical redundancy
- **Protection** – e.g., by physical or electromagnetic hardening.
- **Responsive launch of ISR ('spy') satellites** - highly developed ISR satellites are a key element and in case of conflict a primary attack target. To restore or reconstitute a degraded capability, small modular, preproduced and rapidly ready-to-launch ISR satellites will become more and more important as 'patches' for ISR gaps[114].

4. Concluding Remarks

During Cold War, electronic warfare (EW) was an important military activity; a typical attack method was jamming (disturbance) of communication frequencies and radar signals. After cold war, the focus shifted to network-centric and cyber warfare and drove attention away from traditional EW. But meanwhile, leading powers like United States, Russia and China have significantly upgraded their electronic warfare capabilities. The development of directed energy weapons and the expansion of electronic warfare capacities to outer space by satellites are further reasons for the rapid re-emergence of electronic warfare.

In the United States, electronic warfare and cyber warfare are now integrated in the concept of cyber electromagnetic attacks (CEMA).

The US and Chinese Navy have advanced prototypes of military laser weapons and first reports of real-world attacks exist. The focus of directed energy weapons on Navy ships is not surprising as the size, weight and energy needs of lasers make other applications

[110] Hoehn 2021a and 2021b
[111] Console 2018
[112] Console 2018
[113] Console 2018
[114] Vasen 2018

difficult. A key obstacle of the laser weapon development is the requirement of mobility, but is this restriction really necessary?
High-Powered Microwave weapons are already used in practice to block detonations of improvised explosive devices.
Satellites are of growing strategic relevance to achieve a better global coverage, better imaging quality and faster and more precise analysis and to have a closer relation between threat detection and response. Also, civilian satellite programs expand rapidly. However, satellites and their communication lines are vulnerable for threats like space weather, anti-satellite missiles, co-orbital systems, space debris, but in particular for cyber electromagnetic attacks. The paper has shown that cyber and electronic attacks on satellites are no theory anymore, but already practice. In response, the concept of space resilience was developed as a technical backbone of space defense.
In summary, Electronic Warfare will be an important topic for future warfare concepts.

5. Literature

Abbany, Z. (2020): Modern spy satellites in an age of space wars. Deutsche Welle online 25 Aug 2020 Article a-54691887

ATP 3-12.3 (2019): Army Techniques Publication No. 3-12.3. Headquarters Department of the Army. Washington, DC, 16 July 2019. Approved for public release; distribution is unlimited.

Bundesregierung (2021): Deutscher Bundestag Drucksache 19/27621 19. Wahlperiode 17.03.2021

Cimpanu, C. (2019): NASA hacked because of unauthorized Rapsberry Pi connected to its network. ZDNet 21 June 2019

Console, A. (2018): Space Resilience – Why and How? The Importance of Space Resilience and the Current Approach. Joint Air Power Competence Centre (JAPCC) Journal Edition 27/2018, p.10-16

Cronin, P.M., Neuhard, R.D. (2020): Countering China's Laser offensive. The Diplomat 02 April 2020

CRS (2019): "Space Force" and Related DOD Proposals: Issues for Congress. Congressional Research Service CRS Paper 08 April 2019

Dean, S.E. (2019): US Navy führt Laserwaffen ein. MarineForum 11-2019, p.34-35

Der Reibert (2020): Das Handbuch für die Soldaten und Soldatinnen der Bundeswehr Mittler Verlag.

Die Zeit online (2014): Cyberangriff: Hacker spionierten Luft- und Raumfahrtzentrum aus. 13 Apr 2014

DoD (2018): U.S. Department of Defense, Summary of the 2018 Department of Defense Artificial Intelligence Strategy: Harnessing AI to Advance Our Security and Prosperity

DW (2019): France details military command of space plans to protect satellites. Article a-49747318

Eckel, H.A. (2019): Laser weapon activities in Germany - technology and operational safety aspects. Report of the German Aerospace Center (DLR), Institute of Technical Physics, Stuttgart, 2 pages

EU (2019): EU Space Policy Fact Sheet of the European Commission.

FAZ online (2015): Cyber-Angriff auf TV5 Monde. Ermittler verfolgen Spur nach Russland. FAZ online 09 Jun 2015

Feickert, A. (2018): U.S. Army Weapons-Related Directed Energy (DE) Programs: Background and Potential Issues for Congress. Updated February 12, 2018 R45098

Finkbeiner, A. (2021): Kampf im Orbit. Spektrum der Wissenschaft 17 Mar 2021

FM (Field Manual) 3-36 (2012): Electronic Warfare. Headquarters Department of the Army. Washington, DC, 9 November 2012. Approved for public release; distribution is unlimited.

FM (Field Manual) 3-38 (2014): Cyber Electromagnetic Activities. Headquarters Department of the Army. Washington, DC, 12 February 2014. Approved for public release; distribution is unlimited.

Folmer, K., Margolin, J. (2020): Satellite data suggest Coronavirus may have hit China earlier: Researchers. ABC News online, 08 June 2020

Hlavica, L.K. (2021): Hacker-Attacks Against Satellites. An Evaluation of Space Law in Regard to the Nature of Hacker-Attacks. Master thesis at the Vrije Universiteit Amsterdam, August 2021

Hoadley D.S., Sayler, K.M. (2019): Artificial Intelligence and National Security Congressional Research Service R45178 Version 6 Updated November 21, 2019

Hoehn, J. (2019a): Ground Electronic Warfare: Background and Issues for Congress. September 17, 2019. Congressional Research Service CRS, Document R54919

Hoehn, J. (2019b): U.S. Airborne Electronic Attack Programs: Background and Issues for Congress. May 14, 2019. Congressional Research Service CRS, Document R44572

Hoehn, J. (2021a): Defense Primer: Military Use of the Electromagnetic Spectrum. Updated September 27, 2021. Congressional Research Service CRS, Document IF 11155, Version 12

Hoehn, J. (2021b): Defense Primer: Electronic Warfare. Updated September 29, 2021. Congressional Research Service CRS, Document IF 11118

Hoehn, J. (2021c): Defense Primer: Directed-Energy Weapons. Updated September 29, 2021. Congressional Research Service CRS, Document IF 11882

Hoehn, J.R., Sayler, K.M., Gallagher, J. (2021): Overview of Department of Defense Use of the Electromagnetic Spectrum. Updated August 10 ,2021 R46564

Leithäuser, J. (2015): Aufrüstung für den Krieg der Zukunft. Frankfurter Allgemeine Zeitung No.217/2015, p.4

Magnuson, S. (2021): Navy to Fully Integrate Laser into Aegis Combat System (updated). Navy News 15 Feb 2021 NationalDefensemagazine.org

Marsiske, HA (2016): Bei Strahlenwaffen liegt Deutschland vorn. Article 3117433 Heise.de 25 Feb 2016, 2 pages

Menn, J. (2018): China-based campaign breached satellite, defense companies: Symantec. Reuters online 19 June 2018

Mizokami, K. (2019): The Navy plans to put HELIOS Laser Weapon on Destroyer in 2021.

Morschhäuser, T. (2014): Heftiger Sonnensturm verfehlt Erde nur knapp. Frankfurter Rundschau online version 25 July 2014, p.1-2

NSCAI (2020): National Security Commission on Artificial Intelligence First Quarter Recommendations March 2020, 131 pages

NSTC (2020): Artificial Intelligence and Cybersecurity: Opportunities and Challenges Technical Workshop Summary Report - A report by the Networking & Information Technology Research and Development Subcommittee and the Machine Learning & Artificial Intelligence Subcommittee of the National Science & Technology Council March 2020

Olson, M. (2012): History of Laser Weapon Research. Naval Surface Warfare Center, Dahlgren Division, Corporate Communication, C6,6149 Welsh Road, Suite 239, Dahlgren, VA ,22448-5130 ADA557756 Approved for public release; distribution unlimited

O'Rourke, R. (2021): Navy Lasers, Railgun, and Gun-Launched Guided Projectile: Background and Potential Issues for Congress. Updated October 20, 2021 R44175

OSTP (2020): American Artificial Intelligence Initiative: Year One Annual Report. Prepared by The White House Office of Science and Technology Policy February 2020

Paganini, P. (2015): Turla APT Group Abusing Satellite Internet Links. September 10, 2015 https://securityaffairs.co/wordpress/40008/cyber-crime/turla-apt-abusing-satellite.html

Peck, M. (2021): Airborne Laser Weapons: China's Savvy New Tool. National Interest 21 July 2021

Pekkanen, S.M. (2019): Introduction to the Symposium on the New Space Race. Governing the New Space Race. Ajil Unbound. doi:10.1017/aju.2019.16

Pudo, G., Galuga, J. (2017): High Energy Laser Weapon Systems: Evolution, Analysis and Perspectives. Canadian Military Journal Vol. 17, No. 3, Summer 2017, p.53-58

Rajagopalan, R.P. (2015): Japans Shift in Space Policy Reflects New Asian Realities. 23 Feb 2015

Rajagopalan, R.P. (2019): Electronic and Cyber Warfare in Outer Space. UNIDIR May 2019 — Space Dossier 3, May 2019

Sayler, K.M. (2019): Defense Primer: Emerging Technologies. Updated December 19, 2019. Congressional Research Service CRS, Document IF 11105

Saylor K.M. et al. (2021): Department of Defense Directed Energy Weapons: Background and Issues for Congress. Version 2Updated September 28, 2021, R46925

Strout, N. (2021): National Geospatial Agency (NGA) boss reveals strategy. C4ISRnet.com 06 Oct 2021

The Maritime Executive (2019): Chinas tests laser weapon similar to US Navy prototype. 10 April 2019

Vasen, T. (2018): Responsive Launch of ISR Satellites - A Key Element of Space Resilience? Joint Air Power Competence Centre (JAPCC) Journal Edition 27/2018, p.17-21

von Spreckelsen, M. (2018): Electronic Warfare –The Forgotten Discipline. Why is the Refocus on this Traditional Warfare Area Key for Modern Conflict? Joint Air Power Competence Centre (JAPCC) Journal Edition 27/2018, p.41-45

Weedon, J. (2015): Beyond ‚Cyber War': Russia's use of strategic espionage and information operations in Ukraine. In: Geers, K. Cyberwar in Perspective Russian aggression against Ukraine. NATO CCD COE Publications. Tallinn 2015, p.67-77

Wehner, M. (2016): Cyberkrieg. Frankfurter Allgemeine Sonntagszeitung from 07 Aug 2016, p.6

Weinbaum C., Berner, S. and McClintock, B. (2017): SIGINT for Anyone. The Growing Availability of Signals Intelligence in the Public Domain. RAND Corporation Publication PE273

Yeo, M., Pittaway, N., Ansari, U., Raghuvanshi, V. and Martin, C. (2021): Hypersonic and directed-energy weapons: who has them and who's winning race in Asia-Pacific? The Defense News 15 Mar 2021