2015 7th International Conference on Cyber Conflict:
Architectures in Cyberspace
M.Maybaum, A.-M.Osula, L.Lindström (Eds.)
2015 © NATO CCD COE Publications, Tallinn

Blackout and Now? Network Centric Warfare in an Anti-Access Area-Denial Theatre

Robert Koch
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
robert.koch@unibw.de

Mario Golling
Faculty of Computer Science
Universität der Bundeswehr München
Neubiberg, Germany
mario.golling@unibw.de

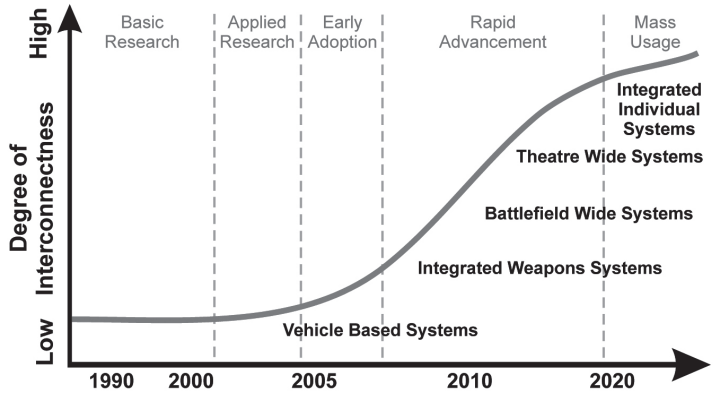
Abstract: The advance of information and communication technology nowadays offers world-wide broadband communication with high data rates. Motivated by the benefits of real-time distributed information shared between units as well as different levels of command for the purpose of fast and reliable decision-making, numerous nations have been working hard over the past years to implement Network Centric Warfare (NCW). By that, information superiority can be gained and translated into command superiority and finally into force superiority. Being strongly dependent on fast and reliable communication, electrical power outages or disruptions of network nodes like SatCom systems respectively links can have a severe impact on information gathering and in turn on the decision making process and the capacity of forces to act. As a consequence, questions arise about the robustness of the NCW doctrine. The ability of power projection is strongly hampered by anti-access/area denial (A2/AD) capabilities. In order to successfully conduct military operations against technologically advanced opponents, forces must address A2/AD as an important element of today's battle-field, comprehend the associated operational implications, and eliminate any imbalances between military objectives and the means by which to achieve them. Following these considerations, this paper - on a technical level - analyses capabilities and weaknesses of NCW with regard to modern theatres. Based on that, recommendations in order to strengthen the performance and reliability for the further development of NCW are given.

Keywords: *Network Centric Warfare, cyber war, A2AD, anti-acess area denial, network breakdown, next-generation military networks, robust NCW.*

1. INTRODUCTION

In recent years, Information and Communication Technology (ICT) has significantly changed our daily life. Today, in one way or another, almost every one of us is affected by ICT. Terms such as Smart Grid, Smart City or Industry 4.0 are only a few examples of how we are dependent on the availability of ICT. Of course, these developments also affect the military. Starting in the early 1990s, the military has been thinking of how the use of ICT can increase the efficiency of forces. One of the first ones who asked themselves how the battlefield of the 21st century will look alike was the US Navy (e.g., see [1]). The main consequence of these considerations is the increased integration of individual, previously autonomously acting systems (see Figure 1). This technical integration has finally led to the concept of Network Centric Warfare (NCW). NCW is a *theory, which proposes that the application of information age concepts to speed communications and increase situational awareness through networking improves both the efficiency and effectiveness of military operations* [2]. As such, NCW creates information superiority by means of a network of reconnaissance, command and control as well as weapon systems and thus ensures the military superiority across the entire range of military operations (full spectrum dominance). The vision for Network Centric Warfare is to provide seamless access to timely information at every echelon in the military hierarchy. This enables all elements, including individual infantry soldiers, ground vehicles, command centres, aircraft and naval vessels, to share information to be combined into a coherent, accurate picture of the battlefield.

FIGURE 1: INTEGRATION OF PREVIOUSLY AUTONOMOUS SYSTEMS IN THE MILITARY (BASED UPON [3])



Proponents argue that the concept of "*strong and flexible network linked military forces*" allows combat units (i) to be smaller in size, (ii) to operate more independently and effectively, (iii) to undertake a different range of missions, (iv) to prevent or reduce fratricides and (v) to speed up the pace of warfare in comparison to non-networked forces [2]. NCW will also produce

(i) improved understanding of higher command's intent, (ii) improved understanding of the operational situation at all levels of command and (iii) increased ability to tap into the collective knowledge of all forces to reduce the "fog and friction" [2]. With the increasing significance, implementation and application of NCW, in particular the following endangerments are rising: Being heavily dependent on the availability and capability of communication between all nodes, the underlying networks represent one of the weakest links of the chain.

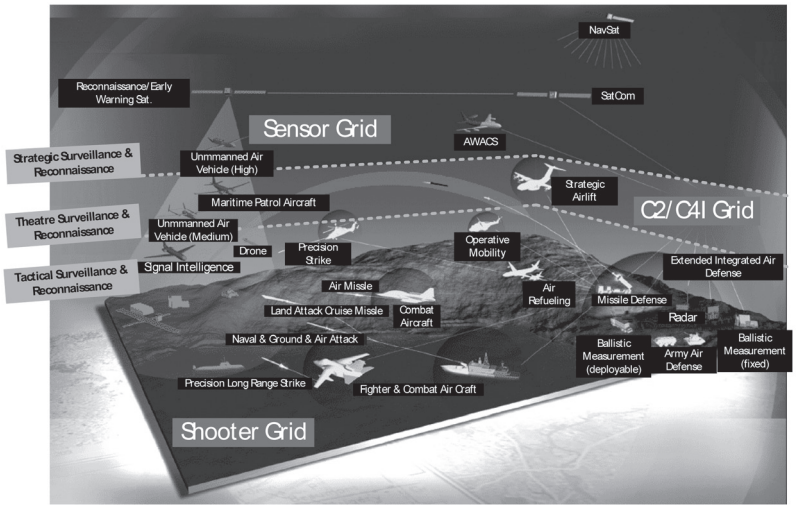
Following these considerations, this paper – on a technical level – analyses capabilities and weaknesses of NCW with regard to modern theatres. On this basis, recommendations in order to strengthen the further development of NCW are given. Therefore, the rest of the paper is structured as follows: First, a deeper introduction into the concept of NCW is given in Section 2. Following this, Section 3 concentrates on the technical capabilities. Here, a brief description of current as well as upcoming technologies and technical trends relevant for communication is given. Section 4 of the paper gives a comprehensive overview of advantages, risks and shortcomings of NCW. Section 5 addresses upcoming advances in ICT. Next to this, Section 6 outlines requirements for the further development of NCW derived from the preceded analysis, supporting the usability of NCW in a contested environment. Based upon that, possibilities for future developments of NCW are described. Finally, Section 7 concludes the paper.

2. THE CONCEPT OF NETWORK CENTRIC WARFARE

The basic element of NCW is gaining information superiority and thereby, command and force superiority by the use of networked sensor grids, high-quality information backplanes, engagement grids and (partly automated) Command and Control (C2) / Command, Control, Communications, Computers, and Intelligence (C4I) processes (see Figure 2) [4].

Vast financial resources have been invested by numerous countries to modernize their ICT and to enable NCW capabilities. Despite these high efforts, this process is currently not completely finished, yet, not even in the US armed forces. While the huge ICT investments of the U.S. DoD already enable information superiority [5], the target structures for full operational capability are not realized completely, yet. For example, the modernization program for tactical networks of the U.S. Army including full networking on-the-move and airborne communication nodes is re-scheduled from 2019 to 2028 [6]. In order to realize a sustainable network structure, open standards and system descriptions are available (e.g., see [7]), motivating industry to develop and provide required systems and components on an affordable base. Furthermore, even with already available ICT capabilities, the NCW theory is often only processed as a transformational concept and has not been adapted extensively to the doctrines, yet. In addition, old-fashioned thinking and resistance to NCW theory hampers an activation of the full power of information superiority [5].

FIGURE 2: WEAPON SYSTEMS, COMMAND AND CONTROL AND A SENSOR GRID ARE INTERCONNECTED WITH ONE ANOTHER TO ALLOW FOR MAXIMUM EFFICIENCY BETWEEN EACH OTHER (ADAPTED ON THE BASIS OF [8])



3. TECHNICAL IMPLEMENTATION OF NETWORK CENTRIC WARFARE

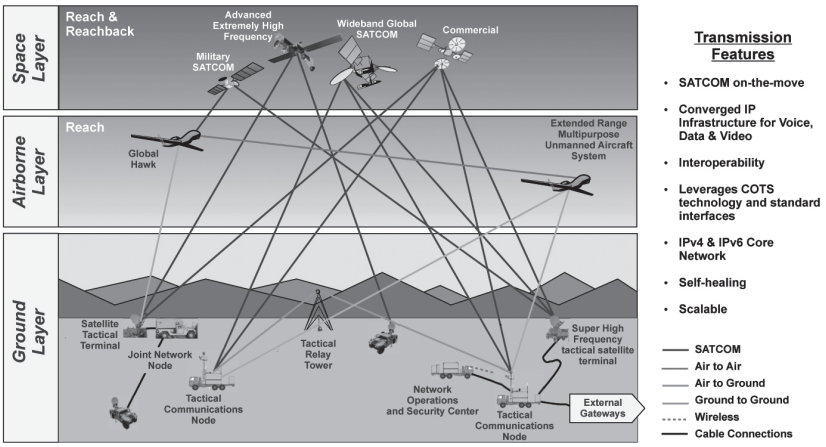
C4I-capabilities are the nervous system of the military. As such, NCW relies on a high-bandwidth communications backbone consisting of fibre optics and satellites, all communicating using the Internet Protocol (IP) [2]. Furthermore, NCW is highly dependent on the interoperability of communications equipment, data, and software to enable networking of people, sensors, and manned and unmanned platforms [2]. Parts of the NCW technology rely on line-of-sight radio transmission for microwave, infrared signals or laser beams and microwave towers, or both low-altitude and high-altitude satellites. The architectures must also have the ability to dynamically self-heal and re-form the network when one or more communications nodes are interrupted [4]. Satellites are crucial for enabling mobile communications in remote areas, as well as for providing imagery, navigation, weather information, a missile warning capability, and a capability to "reach back" to the home country for support [9, 1]. Here, comparatively high requirements are imposed on the data rate. Within the Operation Iraqi Freedom in 2003 for instance, the individual data rate of 64 kilobits per second was considered as too small for the needs of the army [2].

A. Anti-Access Area-Denial (A2/AD)

Modern forces are highly dependent on space assets. As described in a report to the US congress [2], the United States remains highly dependent on space assets, and has enjoyed space dominance during previous Gulf conflicts largely because its adversaries simply did not exploit

space, or act to negate U.S. space systems. In case of a technologically advanced adversary, this dependency created by NCW can therefore result in an Achilles' heel. Forces must be prepared to deploy to a wide range of locations that include almost any type of terrain and confront adversaries that span the threat spectrum from very poorly armed bands to peer-level foes [10]. In this context, the term A2/AD refers to all actions to limit the ability of power projection of an opponent. Anti-access (A2) challenges prevent or degrade the ability to enter an operational area [10]. These challenges can be geographic, military, or diplomatic. Area denial (AD) refers to threats to forces within the operational area [10]. In addition to conventional attacks, in particular AD also includes attacks in cyberspace.

FIGURE 3: SIMPLIFIED MODEL OF A NCW INFORMATION NETWORK (NAVY AND AIR FORCE HAVE BEEN OMITTED FOR SIMPLICITY; IMAGE BASED ON [6])



B. NCW Scenario

For the further analysis of NCW requirements and endangerments, the scenario depicted in Figure 3 will be used; because of the focus of the paper, only technical capabilities are described: Two capable enemies have both realized full operational capabilities of NCW, therefore comprehensively connected units with regard to networks and satellite communication (SatCom) systems.

Both parties possess Electronic Warfare (EW) capabilities in all major subdivisions, namely Electronic Attack (EA), Electronic Protection (EP) and Electronic Warfare Support (EWS). As written in the Joint Publication 3-13.1, "Electronic Warfare" [11], EA is, e.g., the use of electromagnetic energy to neutralize or destroy enemy combat capabilities. EP are actions taken to protect personnel, facilities and equipment from any effects of the use of EM spectrum, while EWS contains actions to search for, intercept, identify and locate radiated EM energy. Therefore, they are able to influence the enemies' actions while protecting the own ones. Both parties are able to execute Computer Network Operations (CNO), namely executing Computer

Network Attacks (CNA) to, e.g., disrupt, deny or destroy information within computer systems and computer networks on the one hand and to protect and monitor networks to detect and respond to network attacks and intrusions by means of Computer Network Defence (CND) on the other hand. See Table 1 respectively Figure 4 for an overview of the different terms. Within a NCW scenario, this presents both, a major chance to manipulate and disrupt systems of the enemy, therefore destroying his NCW capability and hence his information and force superiority. Otherwise, the own dependency on a working NCW system forces a strong protection and capable redundancy to repel attacks of the enemy and keep the superiority.

Beside satellite capabilities, further communication assets can be placed in the airborne layer by the use of, e.g., Unmanned Aerial Vehicles (UAVs). The relevance of secure and capable links can be illustrated with a look at UAVs. E.g., the connection and operation of UAVs requires extensive link capabilities of up to 50 Mbps per unit, where a disruption of the link can have severe effects on the success of the mission. Another example is the use of Special Operation Forces (SOF), which are a strategic asset and therefore heavily dependent on reliable communication links. While link data rates of about 256 to 512 Kbps have been satisfactorily for several years, new sensor technology and an increasing need for extensive data exchange within NCW raise the requirements for data rates dramatically. E.g., while the return link of a Predator UAV started with 3.2 Mbps, a Global Hawk already requires about 50 Mbps today, while possibly reaching 274 Mbps in the near future [15].

FIGURE 4: GRAPHICAL DISTINCTION BETWEEN THE TERMS

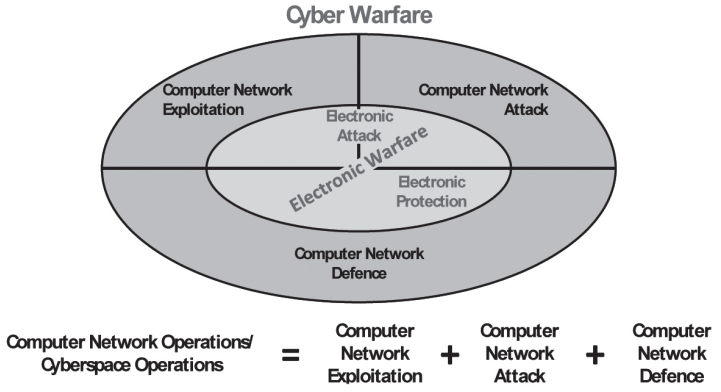


TABLE1: OVERVIEW OF ABBREVIATIONS.

Abbreviations	Definition
Network Centric Warfare (NCW)	Theory that proposes the application of information age concepts to speed communications and increase situational awareness through networking and in turn improves both the efficiency and effectiveness of military operations [2].
Anti-Access (A2)	Corresponds to means which try to prevent or degrade the ability to enter an operational area [10]. These challenges can be geographic, military, or diplomatic.
Area Denial (AD)	Refers to threats to forces within the operational area. AD threats are characterized by the opponent's ability to obstruct the actions of forces once they have deployed [10].
Electronic Warfare (EW)	Refers to any action involving the use of electromagnetic or directed energy to control the electromagnetic spectrum or to attack the enemy. EW includes three major subdivisions: Electronic attack (EA), Electronic Protection (EP), and Electronic Warfare Support (EWS) [11].
Electronic Attack (EA)	The use of electromagnetic energy to neutralize or destroy enemy combat capabilities [11].
Electronic Protection (EP)	Actions taken to protect personnel, facilities and equipment from any effects of the use of EM spectrum [11].
Electronic Warfare Support (EWS)	Actions to search for, intercept, identify and locate radiated EM energy [11].
Cyber Warfare (CW)	The unauthorized conducting of a penetration - including the preparation - by, on behalf of, or in support of, a government into another nations' computer or network, or any other activity affecting a computer system, in which the purpose is to add, alter, falsify or delete data, or cause the disruption of or damage to a computer or network, or the objects a computer system controls (such as SCADA-systems "supervisory control and data acquisition") [12].
Computer Network Operations (CNO) / Cyberspace Operations (CO)	The employment of cyber capabilities where the primary purpose ist to achieve objectives in or through cyberspace [13].
Computer Network Attacks (CNA)	Includes actions taken via computer networks to disrupt, deny, degrade, or destroy the information within computers and computer networks and/or the computers/networks themselves [14].
Computer Network Defense (CND)	Includes actions taken via computer networks to protect, monitor, analyze, detect, and respond to network attacks, intrusions, disruptions, or other unauthorized actions that would compromise or cripple defense information systems and networks [14].
Computer Network Exploitation (CNE)	Includes enabling actions and intelligence collection via computer networks that exploit data gathered from target or enemy information systems or networks [14].

4. THREATS FOR NETWORK CENTRIC WARFARE

As shown before, NCW enables advantages by providing an improved situational awareness of the environment, a better understanding of the operational situation, a dramatically accelerated decision-making as well as a higher mission effectiveness. On the other hand, several risks are inducted by the dependency on capable and reliable communication networks. The decision, if a risk can be taken, depends on a comprehensive risk analysis: if a weakness or vulnerability is indeed existent, but not exploitable by the enemy, it presents no endangerment for the system

respectively operation. Unfortunately, such an absolutely statement is typically not possible in the real-world; often, one only can estimate the risk, e.g., based on intel information, and then decide if the risk can be accepted. For example, the NIST Special Publications 800-39, "Managing Information Security Risk" [16] and 800-30, "Guide for Conducting Risk Assessments" [17], are giving guidance how to establish programs for managing information security risk.

Referring to the scenario, two highly capable enemies are confronted, resulting in high risks that the enemy will attack NCW capacities; vice versa, attacking the enemy's NCW structure can open up an advantageous situation for oneself. Therefore, significant threats to NCW are discussed as follows:

Anti-Satellite: Satellites are fully integrated, essential components of NCW as they are the only systems able to provide a continuous, worldwide broadband network supply. Being placed comparatively secure on different orbital positions, these systems are nevertheless threatened nowadays. The first Anti-Satellite Weapon (ASAT) was launched on May 24, 1962 by the U.S; a shortly ensuing exoatmospheric test of a nuclear ASAT was conducted on July 9, 1962 [18]. After that, the Partial Nuclear Test Ban Treaty (LTBT) from 1963 bans nuclear weapons testing including the atmosphere and outer space, the Outer Space Treaty from 1967 denies the placing of "any objects carrying nuclear weapons or any other kinds of weapons of mass destruction" [19] while the Anti-Ballistic Missile Treaty of 1972 denies the development, test and deployment of ABM systems, inter alia air-based and space-based. The contracts do not deny the development and deployment of ASATs completely; for example, a two-staged anti-satellite missile with infrared homing capability that was air-launched in high altitude from a F-15 was developed in the 1970s [18]. Lately, China demonstrated the relatively simple deployment of a Kinetic Kill Vehicle (KKV), which was engaged by a road-transportable, two-staged CSS-5 rocket and which was used to successfully destroy the Chinese weather satellite Fengyun-1C (FY-1C) on January 11, 2007 [20].

Another endangerment of satellites is the increasing amount of debris: scattered parts of destroyed or broken satellites and systems, rocket firing steps, etc. For example, the destruction of FY-1C produced numerous fragments, now circulating in different orbits. The Space Surveillance Network (SSN, [21]) has registered 3037 objects resulting from the FY-1C collision and scientists of the NASA Orbital Debris Program Office presume 35000 additional objects about 1 cm or more, which are not tracked at the moment [22]. Calculations predict, that only approx. 6% of the fragments of FY-1C will enter Earth's atmosphere until 2017, while 79% will remain in orbit until 2109. Debris presents high risks for the operation of satellites; e.g., the Russian micro-satellite BLITS (Ball Lens in The Space) was hit by a fragment of FY-1C on January 22, 2013 and likely destroyed [23]. Another example is the destruction of the operative communication satellite Iridium 33, which had been hit and destroyed by the non-active Russian communication satellite Cosmos 2251 on February 10th, 2009 [24]. Beforehand, the closest approach of Iridium 33 and Cosmos 2251 was calculated to be approx. 584 m [25], which shows the possibility of error of these methods. The development of new, powerful laser system of reduced sizes (e.g., see [26]) enable the construction and deployment of new ASAT system, but also the design of new protection and active defence capabilities for satellites.

Malicious hard- and software: Because of the steady cutback of defence budgets in most countries after the end of Cold War (the so-called peace dividend), but also in the context of the financial crisis, armament projects are often reduced and financially limited. As a consequence, in-house developments are not possible any longer (besides a few exceptions, e.g., crypto devices) and Commercial, Governmental and Military off-the Shelf (COTS/GOTS/MOTS) products are used comprehensively to reduce R&D and system costs, especially in the area of ICT products. While this reduces costs and enables better performance on the one hand, these products are hardly controllable, fraught with risk to infiltrate highly sophisticated and hardly detectable Trojan circuits and hardware backdoors into high security environments. Especially state-of-the-art weapon systems typically contain numerous COTS components, of which some may include untrustworthy respectively manipulated semiconductors. E.g., see the discussion about hardware backdoor within the Microsemi ProASIC3 (PA3) A3P250 FPGA back in 2012, a programmable logic mainly used in military high-security applications [27], or the public discussion in case of network products from ZTE and Huawei. Other nowadays well-known examples are the ANT products of the NSA, e.g., hardware or persistent firmware backdoors placed in routers, firewalls and servers, providing hardly detectable hidden entries [28]. While the security issues of COTS in defence applications already have been discussed in NATO back in 2000 [29], this was focused on software products.

Because of the increasing endangerment by COTS hardware, more and more research is done with regard to the identification of malicious behaving COTS, e.g., see [30,31]. Current approaches are rarely applicable in practice, e.g., requiring comprehensive information about the circuit diagram, complex and time-consuming procedures or laboratory-style preconditions for their employment. This may open up possibilities to execute an unrecognized backdoor access, to manipulate systems respectively data or to denial of service of satellite links, C2-systems and even weaponry. Within a NCW scenario this is even more dangerous, because one compromised (trusted) node can have severe effects on the whole network. Compared to free enterprise, this reflects the situation of springboard-attacks, where (worse secured) component suppliers are used for the infiltration of highly-secured companies.

Further implications: Beside the described endangerments for satellites and possible weaknesses and vulnerabilities opened up by COTS products, several other threats must be considered. Because of the limited space of this publication and the broader available coverage in literature, they will only be described briefly. In a full operational NCW scenario, attacks on networks and systems can have severe effects on the capacity to act of a party (e.g., see [32]). This enables even a weaker opponent to gain initiative, destroy the superiority of an enemy and therefore, his force superiority. With a strong dependence on communication networks and computer systems, a comprehensive protection is required. The high flexibility of Software Defined Radio (SDR) compared to conventional radio systems makes it attractive for military applications. On the one hand, systems are available at a reduced rate and can be adapted to changing environmental settings and new requirements, e.g., new waveforms can be integrated easily. On the other hand, moving formerly hard-wired system components to software makes them more vulnerable for attacks and manipulation. As SDR and Cognitive Radio, therefore systems that can be programmed and configured dynamically, will act as an important part of NCW, corresponding endangerments have to be considered (e.g., see [33]).

5. UPCOMING ADVANCES IN COMMUNICATION TECHNOLOGY

NCW enables up-and-coming possibilities to gain information and force superiority by using comprehensive and distributed information and networked sensor and effector grids, even with increasingly smaller armed forces. On the other hand, strongly NCW-based operations are endangered by different threats as shown in Section 4. In the following, upcoming advances in communication technology are analysed, which can be used to build up hardened NCW structures, being capable for utilization within an A2/AD scenario.

The major flaw of NCW is the necessity of reliable communication links. Especially SatCom is of central importance for the successful operation; different upcoming techniques can be used and combined, to improve satellite-based links and to add redundancy in case of a denial of satellite services. Because of the limited space, we will handpick some significant advances in transmission technologies, explaining their capabilities and impact on NCW in more detail.

Satellite-based communication: Military satellite networks have been using SHF- and EHF frequency bands extensively since the 1990s. While only very limited data rates had been available in the beginning, also in higher frequency bands (e.g., see [34]), upcoming advances with regard to technology and waveforms provide the capabilities necessary for NCW. For example, todays Ku-band satellites provide data rates of 5 Mbps and above at almost every location on the globe (excluding Polar Regions); with the deployment of Iridium NEXT beginning this year, Ku- and L-band capabilities are available *worldwide* [35]. Because a wide variety of providers and available systems as well as low equipment costs and small terminals, Ku-band is used increasingly by the military of different countries. But also civilian demand increases steadily, resulting in a high utilization of the available capabilities. The theoretical maximum capacity of Ku-band frequencies is nearly exhausted; e.g., the average gap between Ku-band communication satellites over Europe, North America, south-western Asia and Southeast Asia is about 1.5°, not allowing further positioning of additional Ku-band satellites. On the other hand, the expected demand for SatCom capacity in the 2018 is approx. 232 Gbps, resulting in an equivalent bandwidth of 120 GHz within the Ka-band [36]. Ka-band is more influenced by weather effects because of the higher frequencies compared to Ku-band. Vapour, rain, wet snow, clouds in the troposphere and scintillation effects (absorption of electromagnetic energy by various substances and their transformation into short pulses of visible photons [37]) in the ionosphere effect the transmission path and therefore the achievable data rates, e.g., see [38, 39]. Because of improved transmission quality, this band currently experiences an intense growth (e.g., see [40]) after a decline of available resources in the early 2000s [41]. Having clear sky, Ka-band provides approx. four times higher data rates compared to Ku-band. The crossover, where the data rates of Ka-band drop below Ku-band because of rain effects (400 - 800 Kbps), appears about 5% at wet regions when using a satellite dish of 1.3 m [40]. To compensate weather effects affecting the achievable data rates compared to Ku-band systems, Adaptive Coding and Modulation (ACM) can be used to handle weather-induced fading effects of more than 15 dB [38]; in addition, Ka-band antennas are able to achieve higher antenna gains compared to Ku-band antennas.

Airborne communication nodes: While first systems like the Battlefield Airborne Communications Node (BACN) built by Northrop Grumman already have been used in theatre, their necessity and deployment will increase within NCW scenarios. Besides providing additional bandwidth, they can be used to overcome shortcomings of available network capacity as well as make redundant links available, assuring the functionality of NCW in case of malfunctioning satellites. E.g., BACN can be deployed in unmanned as well as manned aircraft and used as "a forward-deployed airborne communications relay and network-centric enterprise information server" [42].

Terrestrial radio communication: HF-based communications with high data rates are under investigation by military as well as civilian institutions. HF frequencies have been used for wireless communication for decades. Because of the low frequency range from 3 to 30 MHz, these bands are very limited with regard to achievable data rates, typically lying between 75 and 9600 Bd (e.g., see [43]); this is not enough for the link requirements of NCW scenarios. While an extension of STANAG 4539 respectively 5066 at the turn of the millennium implemented data rates of 14400 bps with a bandwidth of 3 kHz [44], Appendix D of the revised standard MIL-STD-188-110C now defines waveforms with bandwidths between 3 and 24 kHz and data rates up to 120 Kbps, using 256-QAM [45]. The new waveforms enable real-time video over HF channels as well as the establishment of ad-hoc IP networks; additional extensions allow data rates up to 240 Kbps [46]. Further studies analyse the transport of time-critical email via HF [47] or the use of iterative equalizers for the improvement of transmission quality and speed (e.g., see [48]). While the capabilities of HF channels are, compared to SatCom links, very limited by nature, modern waveforms and technologies enable IP-based real-time communication opportunities. On the other hand, also satellite resources are very limited, resulting in connections of units with often only about 256 Kbps even this very day. The operating experience in handling these limited links with a comparatively large amount of data and the resulting procedures and protocols are the basis for an efficient integration of modern HF links.

Laser-based communication: Techniques for free-space optical data transmission have been investigated since the 1980s, e.g., see [49]. In the meantime, advanced systems for laser-based communication have reached readiness for start of production [50]. For example, the Lunar Laser Communication Demonstration (LLCD) of NASA in 2013 illustrated the use of a pulsed infrared laser for the communication between earth and moon [51]. Over a distance of 385,000 km, the system provided 622 Mbps downlink and error-free 20 Mbps uplink data rates [52]. LLCD is the basis for a flight optical communications terminal, which is going to be placed in geosynchronous orbit in approx. December 2016. Laser-based communication opens up several outstanding advantages, some of particular interest for the military:

- Highly efficient signal encoding nearby the quantum limit, e.g., by using photon-counting techniques
- Highly effective error-correction in case of a lost laser pulse or tampering by noise
- Very high data rates up to 10 Gbps and later, up to Tbps

- Use of optical links in unregulated parts of the electromagnetic spectrum which are invisible for human eye, hardly detectable (e.g., because of the minimal beam of rays, the optical signal is typically only detectable within a radius of a few 10 m around the receiver [53]) and hardly to interfere by enemies
- Utilization of quantum cryptography for additionally securing the link, e.g., see [54]
- Small terminal sizes

Effects like windblown sand and dust atmosphere can have influence on the transmission quality (e.g., see [55]), but projects like LLCD demonstrate the up-and-coming real-world applicability of this technology.

6. ROBUST NETWORK CENTRIC WARFARE

Based on the identified shortcomings and the up-and-coming capabilities of new technology, requirements for Robust Network Centric Warfare (RNCW) are derived as follows.

1. **Computer Network Defence Capabilities:** As confidentiality, integrity and availability of the network is a key element for utilizing NCW, communication links will remain in the focus for attacks even with hardened links. A strong CNA capability can treat even a weak enemy with favour, therefore enforcing strong CND skills for every NCW-depended actor. Because of that, extensive precautions have to be applied and an immediate (“ real-time”) ability to act must be available when suffering attacks or if network and system anomalies are detected. These are especially *organisational* and *financial* aspects of manning, equipment as well as education and training.
2. **Adaptable protocols:** This requirement is addressing layer 2 to 4 of the ISO model. Protocols for data exchange within NCW systems must be able to adapt to changing link capabilities and connection types, e.g., terrestrial communication and radio- respectively laser-based SatCom. Therefore, they must not only be able to adapt the transmission data rate and to intensify error-correction capabilities on unreliable links, but also to split (multiplex) data through multiple transmission paths and networks, while being able to cope with different delays like jitter and latencies at the same time.
3. **Optimized data/ information exchange requirements:** This aspect is addressing *layer 6 and 7* of the OSI model. Modern services and information requirements necessitate the transmission of huge amounts of data. The basic communication structure must be built on a lightweight system, able to transmit all elementary data of the sensor-, C2- as well as shooter grid over an IPv6 network connection with a data rate of 200 Kbps. This enables scooping out all redundancies of a connection mix; an adequate use of vectorised data sets enables the applicability of all available networks, while additional data can be transmitted within free capacity. Therefore, the data exchange has to adapt in an automated manner to the available connection capabilities. E.g., lowering the quality of un-prioritized video streams can be used to optimize available resources while providing enough bandwidth for critical assets, e.g., UAVs executing an attack or data exchange between units required for third-party targeting.

4. **Hardening of satellite systems:** The endangerments for satellites by ASATs and debris as described in Section 4 underlines the need for further hardening of satellite systems as a critical aspect for the reliability of NCW. Several issues have to be addressed (e.g., see [56]):
   - Hardened circuits (e.g., nuclear hardening with regard to electro-magnetic pulses or Gallium Nitride based solid state power amplifiers)
   - Passive self-defence capabilities, e.g., automated collision-detection and avoidance systems,
   - Active self-defence capabilities, e.g., shoot-back equipment or escort satellites
   - Disperse satellite architectures, for example by smaller satellite payloads
5. **Communication networks:** This requirement is addressing *layer 1*, the physical layer. Because of advantages and disadvantages of radio frequencies of different parts of the electromagnetic spectrum, a mix of various segments of the band must be available for every participant within the NCW system. Upcoming technology enables decreasing terminal sizes and mobile equipment for high frequencies (ultra-small aperture terminals), allowing even the single soldier to have access to different networks at any location on the globe. Platforms like vehicles or ships, as a matter of course, have more space for the installation of communication systems. Based on numerous requirements like the positioning of sensors, weapon systems, minimizing of radar cross sections (RCS), etc., also these systems have only very limited opportunities for the installation of, e.g., stabilized SatCom antennas. For a NCW scenario, extensive data rates are required as shown in Section 3. Based on the steady risk of attacks, weather influence and environmental effects which can influence specific frequency bands respectively links significantly, satellite communication has to be provided by an extensive mix of Ku-, Ka- and SHF-bands. Especially upcoming laser-based systems will be a strong enhancement of secure mobile broadband-connectivity. To be able to provide basic communication in case of a complete denial of space- and aerial based systems, terrestrial systems must *still* be able to sustain basic NCW capabilities. This can be realized by including modern waveforms, which enable data exchange up to 240 Kbps even with HF frequencies [46]. While this is still very limited with regard to satellite links with high data rates, it is enough for elementary data exchange.
6. **Airborne communication-nodes:** UAVs providing communication nodes can be used to provide additional as well as redundant and emergency bandwidth and link capability. While these systems have a very limited dwell time with regard to satellite systems, they are highly flexible and can be used on short notice, strongly enhancing the ability to build-up a resistant and dynamic NCW communication network. These nodes are a mainly a capacity enhancement on the physical layer.
7. **Ability to act autonomously for a short period of time:** One consequence of a possible failure of the communication link is that the individual systems should be able to compensate the loss of communication, at least over a limited time window. This should not be limited to fail-safe operation modes, i.e. where the system keeps its current state (like position, altitude, speed, etc.). Instead, the individual system must continue to be able to perform - at least limited - independent actions to achieve the mission goal(s) (semi-autonomous weapons systems). In addition, the need to be

able to operate locally is also increased by the necessity that forces sometimes have to be able to operate without any communication at all (e.g., within a covert/special operation). For completeness, it should be mentioned that, however, this does not imply "Lethal Autonomous Robotics" (LAR), which are activated once and which - without human intervention - aim for enemies and neutralize them (e.g., see [57] for a controversial paper on lethal autonomous targeting).

Based on these recommendations, resistant, capable and adaptable RNCW can be built-up, establishing the prerequisites for successful operations in future theatres.

7. CONCLUSION

Today's western armed forces are getting increasingly efficient while their sizes are still decreasing. This is possible by achieving information superiority and therefore, to dictate the speed of operation and based on that, utilizing force superiority. This kind of operation requires extensive communication processes and data exchange between all assets and all layers; therefore, a strong network infrastructure is required, enabling the use of NCW. Because of the enhancement of technology, core aspects of NCW are endangered highly nowadays, e.g., communication satellites by attacks of ASATs. Therefore, we first identified severe shortcomings and vulnerabilities of today's NCW and second, investigated up-and-coming technologies that can be used to harden NCW. Based on that, we deduced requirements for RNCW, Robust NCW, to enable the ability to counteract the endangerments of an A2/AD theatre.

ACKNOWLEDGMENT

This work was partly funded by FLAMINGO, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Frame-work Programme.

REFERENCES

[1] D. S. Alberts, "Information Age Transformation: Getting to a 21st Century Military (revised)," DTIC Document, Tech. Rep., 2002.
[2] C. Wilson, "Network centric operations: background and oversight issues for congress." DTIC Document, 2007.
[3] Technolytics. Network centric warfare - technology maturity model. [Online]. Available: http://www.directionsmag.com/images/articles/coleman/ncw/ncw3.gif
[4] A. K. Cebrowski and J. J. Garstka, "Network-centric warfare: Its origin and future," in US Naval Institute Proceedings, vol. 124, no. 1, 1998, pp. 28-35.
[5] H. D. Tunnell, "Network-centric warfare and the data-information-knowledgewisdom hierarchy," Military Review, vol. 94, no. 3, p. 43, 2014.
[6] L. Epperson. Satellite communications within the army's win-t architecture. [Online]. Available: http://www.ndia.org/Divisions/Divisions/C4ISR/Documents/492C brief.pdf
[7] U.S. Army CIO/G6, Network Integration Evaluation 15.1 - Technical Architecture. HQDA CIO/G6-AAIC Director, 2013. [Online]. Available: http://ciog6.army.mil/Portals/1/Architecture/NIE_15.1_Technical%20Architecture_and_Appendices.pdf

[8] The Tacticians Database, “Network-centric warfare.” [Online]. Available: http://tactdb.blogspot.de/2014/06/network-centric-warfare.html
[9] D. S. Alberts, J. J. Garstka, and F. P. Stein, “Network centric warfare: Developing and leveraging information superiority,” DTIC Document, Tech. Rep., 2000.
[10] I. Gordon, J. Matsumura et al., “The army’s role in overcoming anti-access and area denial challenges,” DTIC Document, Tech. Rep., 2013.
[11] “Joint Publication 3-13.1, Electronic Warfare,” Joint, Tech. Rep., 2007.
[12] M. Golling and B. Stelte, „Requirements for a Future EWS - Cyber Defence in the Internet of the Future,“ in Proceedings of the 3rd International Conference on Cyber Conflict (ICCC). IEEE, June 2011, pp. 1-16.
[13] J. Cartwright, “Joint terminology for cyberspace operations,” Joint Chiefs of Staff (JCS) Memorandum, 3Nov, 2010.
[14] National Security Agency. Computer network operations. [Online]. Available: https://www.nsa.gov/careers/career_fields/netopps.shtml
[15] http://archive.defensenews.com. Technical briefing: Anatomy of a bandwidth crunch. [Online]. Available: http://archive.defensenews.com/print/article/20090801/C4ISR02/908010313/Technical-briefing-Anatomy-bandwidth-crunch
[16] Joint Task Force Transformation Initiative, “Managing Information Security Risk,” National Institute of Standards and Technology, Special Publication 800-39, March 2011, http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf last visited on May 21th, 2013.
[17] “Guide for Conducting Risk Assessments,” National Institute of Standards and Technology, Special Publication 800-30, September 2012, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf last visited on May 26th, 2013.
[18] G. Marshall. Anti-satellite weapons (asats). [Online]. Available: http://www.space4peace.org/asat/asat.htm
[19] U. N. PUBLICATION, “United nations treaties and principles on outer space (st/space/11),” 2002, sales No. E.02.I.20.
[20] B. Weeden. 2007 chinese anti-satellite test fact sheet. Secure World Foundation. [Online]. Available: http://swfound.org/media/9550/chinese_asat_fact_sheet_updated_2012.pdf
[21] United States Space Command. Space surveillance. O.J. [Online]. Available: http://www.au.af.mil/au/awc/awcgate/usspc-fs/space.htm
[22] T. Kelso, “Analysis of the 2007 chinese asat test and the impact of its debris on the space environment,” 2007.
[23] K. Tate. Russian satellite crash with chinese asat debris explained (infographic). [Online]. Available: http://www.space.com/20145-russian-satellite-chinese-debris-crash-infographic.html
[24] T. S. Kelso, “Analysis of the iridium 33 - cosmos 2251 collision,” 2009.
[25] T. Kelso. Socrates satellite orbital conjunction reports assessing threatening encounters in space. [Online]. Available: http://celestrak.com/SOCRATES/
[26] K. Ludewigt, T. Riesbeck, T. Baumgärtel, J. Schmitz, A. Graf, and M. Jung, “Mobile and stationary laser weapon demonstrators of rheinmetall waffe munition,” in SPIE Security+ Defence. International Society for Optics and Photonics, 2014, pp. 92 510N-92 510N.
[27] S. Skorobogatov and C. Woods, Breakthrough silicon scanning discovers backdoor in military chip. Springer, 2012.
[28] J. Appelbaum, J. Horchert, and C. Stöcker. Catalog advertises nsa toolbox. SPIEGEL ONLINE 2013. [Online]. Available: http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994-druck.html
[29] NATO Research and Technology Organisation, “Commercial off-the-shelf products in defence applications (the ruthless pursuit of cots),” in Information Systems and Technology Panel (IST-016). NATO, 2000.
[30] S. Wei and M. Potkonjak, “Scalable hardware trojan diagnosis,” Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 20, no. 6, pp. 1049-1057, 2012.
[31] R. Rad, J. Plusquellic, and M. Tehranipoor, “A sensitivity analysis of power signal methods for detecting hardware trojans under real process and environmental conditions,” Very Large Scale Integration (VLSI) Systems, IEEE Transactions on, vol. 18, no. 12, pp. 1735-1744, 2010.
[32] J. Rantapelkonen, M. Salminen et al., “The fog of cyber defence,” Julkaisusarja 2. Artikkelikokoelma n: o 10, 2013.
[33] A. Banerjee and S. Das, “A review on security threats in cognitive radio,” in Wireless Communications, Vehicular Technology, Information Theory and Aerospace Electronic Systems (VITAE), 2014 4th International Conference on, May 2014, pp. 1-5.
[34] Comparison of milsatcom systems. [Online]. Available: http://www.fas.org/spp/military/docops/army/reftext/chap07b.htm
[35] O. Gupta and C. Fish, “Iridium NEXT: A Global access for your sensor needs,” AGU Fall Meeting Abstracts, p. A663, Dec. 2010.

[36] ECC, “The use of the frequency bands 27.5-30.0 GHz and 17.3-20.2 GHz by satellite networks,” Electronic Communications Committee (ECC) within the European Conference of Postal and Telecommunications Administrations (CEPT), Tech. Rep. ECC Report 152, 2010.
[37] Scintillation Materials Research Center. What are scintillation materials? [Online]. Available: http://www.engr.utk.edu/smrc/
[38] J. Petranovich, “Mitigating the effect of weather on ka-band high-capacity satellites,” 2012.
[39] A. Dissanayake, “Ka-band propagation modeling for fixed satellite applications,” Online Journal of Space Communication, vol. 2, pp. 1-5, 2002.
[40] D. Brunnenmeyer, S. Mills, S. Patel, C. Suarez, and K. Ling-Bing, “Ka and ku operational considerations for military satcom applications,” in Military Communications Conference, 2012 - MILCOM 2012, Oct 2012, pp. 1-7.
[41] O.V., “Global analysis of satellite transponder usage and coverage,” 2003.
[42] J. Lamar. Northrop grumman airborne communications system wins award for outstanding industry achievement. Northrop Grumman Information Systems. [Online]. Available: http://www.irconnect.com/noc/press/pages/news releases.html?d=184859
[43] M. Uysal and M. Heidarpour, “Cooperative communication techniques for futuregeneration hf radios,” Communications Magazine, IEEE, vol. 50, no. 10, pp. 56-63, October 2012.
[44] A. Gillespie and S. Trinder, “Performance characteristics of high data rate hf waveforms,” in HF Radio Systems and Techniques, 2000. Eighth International Conference on (IEE Conf. Publ. No. 474), 2000, pp. 335-339.
[45] Department of Defense, “Interoperability and performance standards for data modems,” Tech. Rep. Department of Defense Interface Standard, 2011.
[46] M. Jorgenson, R. Johnson, and R. Nelson, “An extension of wideband hf capabilities,” in Military Communications Conference, MILCOM 2013 - 2013 IEEE, Nov 2013, pp. 1201-1206.
[47] M. Oezdemir, A. Eliacik, I. Guenes, and A. Sasioglu, “Time-critical e-mail transfer over hf radio,” in European Wireless 2014; 20th European Wireless Conference; Proceedings of, May 2014, pp. 1-6.
[48] M. Elgenedy, E. Sourour, and M. Nafie, “Iterative mmse-dfe equalizer for the high data rates hf waveforms in the hf channel,” in Signals, Systems and Computers, 2013 Asilomar Conference on, Nov 2013, pp. 1243-1247.
[49] V. Rampal, “Blue green lasers and their military potential,” Defence Science Journal, vol. 33, no. 2, pp. 183-193, 1983.
[50] S. Magnuson. (2013) Game-changing laser communications ready for fielding, vendors say. National Defense Magazine. [Online]. Available: http://www.nationaldefensemagazine.org/archive/2013/January/Pages/Game-ChangingLaserCommunicationsReadyForFielding,VendorsSay.aspx?PF=1
[51] B. L. Edwards, D. Israel, K. Wilson, J. Moores, and A. Fletcher, “Overview of the laser communications relay demonstration project.” [Online]. Available: http://www.spaceops2012.org/proceedings/documents/id1261897-paper-001.pdf
[52] J. Buck. Nasa laser communication system sets record with data transmissions to and from moon. [Online]. Available: http://www.nasa.gov/press/2013/october/nasa-laser-communication-system-sets-record-with-data-transmissions-to-and-from/
[53] D. Giggenbach, “Mobile optical high-speed data links with small terminals,” in SPIE Europe Security+ Defence. International Society for Optics and Photonics, 2009, pp. 74 800I-74 800I.
[54] R. J. Hughes, W. T. Buttler, P. G. Kwiat, S. Lamoreuax, G. Morgan, J. E. Nordholt, and C. G. Peterson, “Quantum cryptography for secure satellite communications,” in Aerospace Conference Proceedings, 2000 IEEE, vol. 1. IEEE, 2000, pp. 191-200.
[55] Y. Ruike, H. Xiange, H. Yue, and S. Zhongyu, “Propagation characteristics of infrared pulse waves through windblown sand and dust atmosphere,” International Journal of Infrared and Millimeter Waves, vol. 28, no. 2, pp. 181-189, 2007. [Online]. Available: http://dx.doi.org/10.1007/s10762-006-9186-4
[56] Harrison, Todd, “The Future of MILSATCOM,” Center for Strategic and Budgetary Assessments, CSBA Study, July 2013.
[57] N. Sharkey, “Saying `no!’ to lethal autonomous targeting,” Journal of Military Ethics, vol. 9, no. 4, pp. 369-383, 2010.