Denkwürdigkeiten

Journal der Politisch-Militärischen Gesellschaft

Nr. 111
Februar 2019

Herausgegeben vom Vorstand der Politisch-Militärischen Gesellschaft e.V. (pmg) in Berlin

ISSN 1436-3070

LEADOFF

Liebe Mitglieder,

durchaus bunt, aber zugleich vollkommen losgelöst vom rheinischen Karneval zeichnet diese 111. Ausgabe der Denkwürdigkeiten das komplexe Bild hybrider Herausforderungen zu Land, in der maritimen Domäne wie auch im Weltraum. Es wird nicht einfach, damit erfolgreich umzugehen.

Wer Schock und Dauerbelastung gut überstehen oder – besser noch – erst gar nicht erleben will, muss dafür dringlich, umfassend und hart arbeiten. Das Spektrum reicht vom Verstehen bis hin zum Gestalten. Vieles ist zu tun. Die Dynamik ist groß. Gelegentlich entsteht der Eindruck, als ob sich Autokratien wie China, Russland und Singapur auf hybride Herausforderungen leichter und besser einstellen als Demokratien.

Ralph Thiele, Vorstandsvorsitzender

In dieser Ausgabe

THEMEN

Wie weiter in Afghanistan?

Die Ankündigung Präsident Trumps, die US-Truppen zügig aus Afghanistan abzuziehen, wird für die deutsche Präsenz am Hindukusch unmittelbare Folgen haben. Steht der längste Einsatz deutscher Kontingente seit dem 30jährigen Krieg kurz vor dem Ende? Wie sind die Aussichten für eine Verhandlungslösung?

Die nachfolgende Analyse beruht auf Feststellungen eines internationalen Kolloquiums, das am 2. Februar 2019 in der Nähe von New York stattfand.

Gesamtlage

Die politische, militärische und ökonomische Lage Afghanistans hat sich 2018 weiter verschlechtert. Aber sie darf nicht negativ überzeichnet werden. Nach dem weitgehenden Rückzug der ausländischen Stabilisierungskräfte hat sich in großen Teilen des Landes auf lokaler und regionaler Ebene ein labiles Gleichgewicht zwischen den verschiedenen ethnischen, religiösen und politischen Gruppierungen gebildet.

Dies ändert allerdings nichts daran, dass Afghanistan ein höchst fragiler Staat bleibt, der ausländischer Stabilisierung bedarf. Die afghanischen Sicherheitskräfte sind abgekämpft. Ohne Finanzierung und Rückendeckung von außen sind sie nicht durchhaltefähig.

Kabul bleibt Ziel von Attentaten und Anschlägen. Die Städte Masar e-Scharif, Herat und im Süden auch Kandahar erfüllen weiter ihre Aufgaben als regionale Zentren. Als kritisch wird die Lage im Südwesten und vor allem im Osten beurteilt. Die „paschtunisch-segmentäre Gesellschaft“, so ein VN-Experte, verhindert in der Stadt Dschalalabad den Aufbau einer auch nur annähernd funktionierenden Verwaltung und macht die Provinz Nangahar zu einem Rückzugs- bzw. Operationsgebiet des IS.

In der Provinz Ghazni kam es im August 2018 zu einer gezielten Offensive der Taleban gegen die schiitischen Hazara. Möglicherweise war diese Offensive auch ein Warnsignal an die Adresse Teherans. Im Südwesten Afghanistans dagegen arbeiten Tale-

ban-Gruppierungen mit iranischen Stellen zusammen, insbesondere beim Drogenschmuggel über die afghanisch-iranische Grenze. Der Norden des Landes bleibt weiter relativ ruhig.

Der politische Kalender 2019

Wichtigstes innenpolitisches Ereignis des Jahres 2019 wird die Wahl eines neuen afghanischen Präsidenten. Ursprünglich für April vorgesehen, soll die Wahl nun im Sommer 2019 stattfinden.

Die VN rechnen jedoch mit einer weiteren Verschiebung bis Ende September. Das Kalkül Präsident Ghanis sehe vor, seine politischen Gegner durch eine Verlängerung des Wahlkampfes finanziell ausbluten zu lassen, während er als Staatspräsident und Regierungschef weiterhin Zugriff auf staatliche Ressourcen behält. Zur Haushaltslage wurde ergänzend bemerkt, dass durch Reorganisationsmaßnahmen unter Präsidenten Ghani gegenwärtig höhere Zolleinnahmen an die Zentralregierung fließen als in der Vergangenheit.

Dem „Ticket" Präsident Ghanis mit Amrullah Saleh, dem früheren Geheimdienstchef, und Justizminister Sarwar Danesh, einem Hazara, steht ein von vom früheren Innenminister und Nationalem Sicherheitsberater Hanif Atmar geführtes starkes Team mit Yunus Quanuni und Karim Khalili, beides ehemalige Vizepräsidenten, gegenüber. Allerdings gibt es in der politischen Elite Kabuls weiterhin Intrigen und Streitigkeiten, so dass die endgültige Zusammenstellung der Kandidatenlisten abgewartet werden muss.

Vor allem aber hängt der politische Kalender vom weiteren Verlauf der Gespräche mit den Taleban und der sicherheitspolitischen Lagenentwicklung ab. Eine Frühjahrsoffensive der Taleban im Mai 2019 wird erwartet.

Gespräche mit den Taleban

Die Gespräche mit den Taleban werden auf zwei unterschiedlichen Verhandlungssträngen geführt. Der eine wird von Moskau über den Sondergesandten Zamir Kabulow, der andere von Washington über Zalmay Khalilzad geführt.

Der Kabulow-Ansatz ist multilateral und bezieht hochrangige Afghanen, die in der Vergangenheit zu den Gegnern der Taleban gehörten, mit ein. An den Gesprächen unter Leitung Kabulows sind Vertreter der folgenden Staaten beteiligt: China, Indien, Pakistan, Iran und die zentralasiatischen Nachbarn Afghanistans. Bei einem der letzten Treffen in Moskau waren auch die USA durch einen Beobachter der dortigen US-Botschaft vertreten. Außer den Taleban nehmen an den Gesprächen hochrangige Angehörige innerafghanischer Gruppen teil, die zu den politischen Gegnern Präsident Ghanis gerechnet werden. Für ein Treffen in Moskau am 5. Februar 2019 hatten der frühere Präsident Hamid Karzai, der Tadschike Atta Mohammad Noor, früher Gouverneur der Provinz Balkh, und der Führer der schiitischen Hazara-Partei Wahdat, Mohammad Mohaqeq, ihre Teilnahme zugesagt.

Der Khalilzad-Verhandlungsstrang ist bilateral angelegt. Khalilzad verhandelt als Sondergesandter für die USA mit den Vertretern der Taleban in Doha. Anschließend informiert er die Regierung in Kabul. Es gibt Anzeichen dafür, dass Khalilzad auch Saudi-Arabien und die VAE über den Verlauf der Gespräche unterrichtet. Die nächste Runde der US-Gespräche mit Taleban-Vertretern soll am 25. Februar 2019 in Doha stattfinden. Nach Auffassung von Experten handelt es sich bei den Taleban, die bisher mit Khalilzad in Doha sprachen, um nachrangige, weisungsgebundene Vertreter („messenger boys").

Der weitere Verlauf der Gespräche auf den beiden Verhandlungssträngen ist schwer zu prognostizieren.

Regionaler Kontext

Bei der Beobachtung und Bewertung der weiteren Entwicklung ist der regionale Kontext einzubeziehen, insbesondere das Verhältnis der USA zu Iran. Es gibt Hinweise darauf, dass sich die Taleban bereit erklären könnten, einer weiteren Stationierung von US-Streitkräften auf den Luftwaffenstützpunkten Bagram und Shindand zuzustimmen. Ebenso gibt es Anzeichen dafür, dass private US-Sicherheitsdienstleister im Westen und Südwesten Afghanistans eine verstärkte Rolle spielen.

Bemerkenswert erscheint schließlich, dass durch den von Indien finanziell geförderten Ausbau einer vierspurigen Teerstraße im Nordteil der westafghanischen Provinz Nimroz eine Allwetter-Straßenverbindung zum iranischen Hafen Chabahar hergestellt werden konnte. Sie führt von dort über Iranshar, Zahedan, Zaranj zur afghanischen Ringstraße und von dort über Herat nach Norden zum Terminal der turkmenischen Eisenbahn und damit zum Eisenbahnnetz Zentralasiens. Der Landtransport vom Indischen Ozean nach Zentralasien wird damit erheblich verkürzt. Karachi verliert als Umschlaghafen an Bedeutung. Die US-Treasury hat für Einfuhren nach Afghanistan über den iranischen Hafen Chabahar eine generelle Befreiung von den US-Sanktionen erteilt („blanket or summary waiver").

asiaticus

THEMEN

Russland: Rückgang des Realeinkommens

Am 25. Januar 2019 berichtete die russische Statistikbehörde ROSSTAT, dass das Realeinkommen im Jahr 2018 um 0,2% gesunken ist, selbst unter Berücksichtigung der Zahlung von 5.000 Rubel (67 €) an die Rentner im Januar 2017.[1] Das ist bereits das fünfte Jahr mit einem Rückgang des persönlichen Einkommens hintereinander. In der jüngeren Geschichte Russlands ist ein so langer Rückgang bisher nicht eingetreten, selbst in den 1990er Jahren nicht, so Kirill Tremassow, Direktor der Analytischen Abteilung von „Loko-Investa". (Im Jahr 2014 war das

[1] www.vedomosti.ru/economics/articles/2019/01/25/792487-dohodi-rossiyan

Realeinkommen um 0,5% gesunken, 2015 um 4,1%, 2016 um 5,6% und 2017 um 1,2%.) Angesichts der Zunahme der Inflation, der Steueranhebung und der angespannten Fiskalpolitik besteht kein Zweifel, dass das Realeinkommen auch 2019 weiter sinken wird, so prognostiziert er.

Der Chef des Rechnungshofs der Russischen Föderation, Alexej Kudrin, und wichtige Minister hielten am 15. Januar 2019 auf der Wirtschaftskonferenz des Gajdar-Forums in Moskau die Erreichung eines der Hauptziele von Präsident Putin in dessen Erlass vom Mai 2018, den Eintritt Russlands in die fünf wichtigsten Volkswirtschaften der Welt mit einer jährlichen Wachstumsrate von 3-4%, für fast unmöglich.[2] Kudrin bestand auf institutionellen und strukturellen Reformen, darunter der Schwächung der vom föderalen Zentrum geschaffenen Machtvertikale.

Bei einer Umfrage von 1.600 Personen über 18 Jahren in 136 Bevölkerungspunkten (Städten, Dörfern usw.) in 52 Föderationssubjekten (Gebieten, Republiken usw.) vom 13. bis 19. Dezember 2018, deren Ergebnisse das Moskauer Meinungsforschungsinstitut Lewada-Zentrum am 14. Januar 2019 veröffentlichte, sprachen sich 53% für den Rücktritt der Regierung aus (im November 2016 waren es 33%).[3] 57% der Befragten warfen der Regierung vor, dass sie die Preiserhöhungen und den Rückgang des Realeinkommens nicht stoppen. Laut einer Umfrage des Moskauer Meinungsforschungsinstituts WZIOM vom 9. bis 13. Januar 2019 billigen nur 35% die Tätigkeit von Premier Dmitrij Medwedew und 39,5% der Regierung.[4]

Putin vertrauen lediglich 33,4% (Anfang Dezember 37%), die Tätigkeit des Präsidenten befürworten nur noch 62,1% (Dezember 64,6%) und der Machtpartei „Einiges Russland“ 33,8%. Die Gründe für den Vertrauens-verlust dürften die Erhöhung des Renteneintrittsalters, die Mehrwertsteueranhebung und die Steigerung der Kommunalausgaben sein.[5]

Der Vorsitzende der Staatsduma, Wjatscheslaw Wolodin, erklärte am 21. Januar 2019, dass es notwendig sei, die bestehenden Defizite der Verfassung zu beseitigen, die mit dem „Mangel an einer angemessenen Balance im System der Kontrolle und des Gleichgewichts der Regierungszweige, zugunsten der Exekutive“ verbunden sind.[6] Die Macht verliere an Ratings, und das hänge hauptsächlich mit dem sozialen Wohlbefinden der Gesellschaft zusammen. Die Gesetzgebung müsse die „Definition des Sozialstaats zutreffender offenlegen“. Die Verfassungsrichterin Tamara Morschtschakowa verband den Vorschlag Wolodins teilweise damit, dass „*etwas getan werden muss, um zu verhindern, dass das Rating der Regierung weiter fällt. Die Lage der Menschen ist sehr schlecht*.“.

Prof. Dr. Eberhard Schneider

Prof. Dr. Lic. Eberhard Schneider ist Vizepräsident der International Union of Economists St. Petersburg (IUECON) sowie Advisory Board Member des EU-Russia Centre in Brüssel, Professor für Politikwissenschaft an der Universität Siegen und Leiter der sozialwissenschaftlichen Forschung des Berliner West-Ost-Instituts.
Der Beitrag erschien erstmalig in ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 599, Februar 2019.
www.ispsw.de

THEMEN

Game Changer Cyber: Towards New Economics of Space?

Hybrid & Disruptive

Hybrid threats and disruptive technologies are shaping a diverse, and fast-developing strategic environment in which an increasing number of relevant actors builds their security strategies on the rule of force.

A clear and memorable visualisation of the term hybrid threats occurred in the Russian use of little green men. These were soldiers in unmarked green army uniforms, carrying modern Russian military weapons and equipment that appeared during the Ukrainian crisis of 2014. These and other hybrid threats have blurred the traditionally understood division between conventional and unconventional threats. They combine: high-tech and low-tech weaponry; new strategies and tactics; a wide and confusing array of state and non-state combatants; overlapping political, criminal, economic and terroristic methods and agendas; as well as multiple informational techniques, including traditional and social media.

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

Satellite Communications (SATCOM) can be expected to be a crucial backbone of evolving global communications networks, as they deliver the information needed for comprehensive situational awareness. SATCOM are key enablers for civil and military missions in particular in remote and austere environments with little or no infrastructure. They are critical for defence, security, humanitarian aid, emergency response, and diplomatic communications.

Cyber has emerged as the absolute and unsurpassed enabler of hybrid threats posed by government agencies and non-state actors. The time when cyber was

[2] www.ng.ru/economics/2019-01-16/4_7483_econ1.html
[3] www.levada.ru/2019/01/14/deyatelnost-pravitelstva-2/
[4] https://wciom.ru/index.php?id=236&uid=9518
[5] www.vedomosti.ru/opinion/articles/2019/01/22/792043-putina
[6] www.kommersant.ru/doc/3860143

simply an emerging capability that needed to be exploited is long gone. Today cyber has become a game changer in multiple domains. It has evolved into a global domain consisting of the interdependent networks of information technology infrastructures and resident data. This includes the internet, telecommunications networks, and computer systems. Equally, it has significant influence on other domains, such as land, air, sea, and space.

Perhaps one of the most challenging of potential scenarios – actually one currently confronting NATO and the European Union – is an opponent's ability to establish Anti-Access/Area Denial (A2/AD) postures, i.e. an opponent's ability to counter one's own power projection, blocking freedom of manoeuvre in key areas. The unhindered access to – and freedom to operate in – space is of vital importance to nations and international organisations, such as NATO and the European Union. Navigation and weather monitoring, communications and financial networks, military and intelligence systems – all of these and more have components in the space domain.

Space infrastructure has become a critical infrastructure. As technologies are expanding, transforming space activities, government actors, and companies are adapting to the new status quo, and goalposts are shifting. Some states have developed the capacity – from space or from Earth, by cyber, manoeuvres or even by force – to prevent access to space, or to degrade the space capabilities of other countries. Today, the space environment, much like the cyber environment, is particularly vulnerable to hybrid threats, such as spying or interrupting services. This constitutes a grey zone of predominantly covert aggression. Given that there are few distributed technological systems that do not rely on satellites for some vital piece of their functionality, the importance of space assets and retaining the confidentiality, integrity, and availability of the information that they carry cannot be overstated. It is, thus, evidently of concern that space assets have not been properly protected against cyber-attack.

NEO & MEO

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

Security organisations and armed forces have structured a new business model on modern, interoperable, scalable and service-oriented IT. Its core and support processes are Command, Control, Communications, Computers, and Intelligence (C4I). These serve as an indispensable basis for Network Enabled Operations, networking relevant actors, units and facilities, as well as linking sensors and effectors together.

In future, security organisations and armed forces will control and coordinate many processes in real time and over long distances. To this end, the standardisation and modularisation of many individual process steps is important. As is the programming of virtually editable models of these modules. Such actions are key in order to plan, control and monitor both organisational and operational processes. Meanwhile, AI and Big Data permit the evaluation and operational/logistical use of the mass data collected.

C4I delivers situational awareness when and where it's needed to support decision-making. This real-time situational awareness vastly increases the agility of forces to manoeuvre and respond. Communication is the fundamental component of C4I. Satellite systems provide C4I with a maintenance-free medium. As such, they have become the backbone which enables high mobility, quick deployment, wide geographical coverage, and independence of terrestrial infrastructure. They deliver secure high bandwidth and ubiquitous coverage, enabling highly scalable content distribution, as well as connecting fixed and on-the-move 5G network sites. Consequently, space capabilities have become central to NEO, including missile warning, geolocation and navigation, target identification, and tracking of adversary activities. Opponents understand this well. Space has become their centre of gravity for downgrading C4I.

On the industrial side the digitalisation of industry and economy drive growth. As such, the space industry benefits from advanced capabilities, business models and services. Industry 4.0 is revolutionising collaboration, production and services, as well as the fundamentals of successful competition. It provides the emerging environment in which computers and automation come together in a new way with remotely connected robotics, guided by computers equipped with AI. This allows for the learning of algorithms, which permits robotics control and adaptation with very limited human interface. As NEO intend the coherent integration of information systems to achieve enhanced military effect the integrity of networks in critical infrastructure sectors such as space is crucially important.

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

The defence and security community has recognised the powerful capabilities of these emerging constellations in enabling NEO. The closer proximity of LEOs and MEOs to Earth allows them to deliver ultra-high bandwidth with much less delay as compared to Geostationary Orbit (GEO) satellites. MEOs and LEOs support real-time command-and-control applications, including transporting Unmanned Aerial Vehicle (UAV)

Intelligence, Surveillance and Reconnaissance (ISR) data from an area of operation to analysis centres in respective headquarters anywhere in the world. Secure embassy communications, police, intelligence and special forces requirements are other perfect fits. The SES-owned MEO is already performing in orbit, thus bringing new capabilities to a variety of users. Others will follow.

In particular small satellites have triggered the interest of the communication-based service sector. They could, for instance, be of use with regard to the Internet of Things, machine-to-machine data exchange using the automatic identification system (AIS), and when tracking aircraft in flight. With its faster speed, lower latency and higher bandwidth, 5G holds the future of the Internet of Things. 5G combines hardware and software more than any of its predecessors. Consequently, software is inherently vulnerable to cyberattacks, if easier to update and replace; hardware is harder to replace if compromised, although international standards are emerging.

The commitment to realising novel approaches by key operators has driven innovation. The technological advancement – from within the industry and beyond – demands the sector's constant evolution. New players are finding opportunities to deploy communications systems which diverge from the pre-existing models of their competitors. Taken as a whole, this drives the emergence of new markets and space-based business models. Governments, commercial customers and industry should all prepare themselves for new business models and the new economics of space. While there is already significant change in the space industry, there is still much more to come. The stage has been set for a rapidly expanding and highly interactive space-based economy moving forward, with cyber as a key driver.

Actors & Vectors

Cybersecurity threats to space infrastructure are a relatively new phenomenon. For a long time, space used to be an ecosystem of its own. As longstanding technological and cost barriers to space have fallen, more countries and commercial firms have begun participating in satellite construction, space launch, space exploration etc. Along with these developments, both new opportunities and new risks for space-enabled services have emerged. Today, with the sophisticated knowledge garnered from satellite command & control and data distribution networks, it is increasingly understood that space assets have been far too vulnerable to cyberattack. Actors can use offensive cyberspace capabilities to enable a range of reversible to nonreversible effects against space systems.

Florence Parly, French Minister of the Armed Forces, highlighted recently: "Cyber capabilities have become … (an) … important asset to impact on … spacecraft or their control centres and ground stations and interrupt their service and functionality."[7] Unfortunately, cyber threats are very hard to detect, and even when discovered, it is difficult to pinpoint and hold responsible the actors behind such attacks.

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

China has supported cyberespionage against U.S. and European satellite and aerospace industries for over a decade.[8] It has been targeting network-based C4I, logistics, and commercial activities. It also plays a role in cyberespionage targeting foreign space entities, industrial and technical intellectual properties.

There is a legacy of Russian cyber-attacks. For example in 2015, a Russian group of hackers with connections to Russian intelligence hijacked unencrypted commercial satellite connections in order to steal data. Similarly, North Korea and Iran have advanced cyber capabilities, along with a history of attacking international assets in the cyber domain.

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

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

[7] Florence Parly. French Minister of the Armed Forces. Remarks on Space & Defence at the French space agency's Toulouse headquarters. September 7th, 2018. Posted in English translation on 23 September 2018 by gosnold https://satelliteobservation.net/2018/09/23/space-defence-policy-speech-by-the-french-ministry-of-the-armed-forces/

[8] DIA. Challenges to Security in Space. January 2019. www.andrewerickson.com/wp-content/uploads/2019/02/DIA_Space-Security-Challenges_201901.pdf

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

Against this backdrop, cyber situational awareness has to deliver inputs based on a common sharable cyber operational picture. A designated common cyber operational picture needs to synthesise the current performance of cyber systems and operations, as well as current threats into an integrated picture. It reports status, vulnerability, threats, suspicious activity, and mission impact. It provides real-time information to tactical, operational and strategic decision-makers.[9]

Cybersecurity Beyond Earth

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

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

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

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

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

Transferring the upcoming hybrid and disruptive technological challenges into a viable, security/defence capability that also pays off on European and global markets is the core of the upcoming cybersecurity challenge. Improving space cybersecurity requires extending good cybersecurity practices into the commercial space sector and addressing problems specific to space activities. Advice for this sector repeats familiar mantras, such as the need for intra-sector collaboration, information sharing, enterprise risk management, encryption, insider threat prevention, and supply chain protection.

To get there, an innovative ecosystem is needed where frogs & eagles grow well. We must develop innovative, courageous, highly capable engineers, specialists and professionals. We must foster small and medium-sized companies (SMEs) that master technological cyber challenges while driving innovation and disruptive technologies. We also need generalists and decision-makers that understand and orchestrate complex, dynamic systems. We need Lead System Integrators (LSIs) that master the orchestration of high-tech solutions into an interoperable, superior network-

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

enabled system, thus facilitating better security and better business.

Ralph Thiele

Ralph D. Thiele is Chairman of the Political-Military Society (pmg), Berlin, President of EuroDefense Germany, Germany and CEO at StratByrd Consulting.
This paper was first presented at the GOVSATCOM Conference, 14.02.2019in Luxemburg.
Opinions expressed in this contribution are those of the author.

THEMEN

Maritime Hybrid Risks and Threats

Consequences for Harbours, Navies and Maritime Services – A European View

"People only accept change in necessity and see necessity only in crisis."
Jean Monnet

"*The international consensus on 'hybrid warfare' is clear: no one understands it, but everyone, including NATO and the EU, agrees it is a problem*".

Introduction

The raison d'être of ports is interconnection. Ports play a pivotal role in international maritime trade and passenger transport. Some ports act as specialized nodes for international container traffic, while others are terminals for the transfer of goods or passengers between the hinterland and other ports, switching transport modes. Oil and gas terminals are in a different category often more distant from built-up areas. Pipelines provide the interlinkages.

Ports often occupy a wide sea area including anchorages, pilot stations and waiting areas which are all potentially open to attack, with the ships clearly visible, stationary and without obvious protection.

The global shipping industry – much like air, road and rail transportation – is undergoing a technological revolution. Automation has made incredible advances in recent years and will continue to do so.

"Ships are an opening to the outside world," wrote Chris South, a senior underwriter for West of England Protection and Indemnity (P&I) Club.

"Four factors are at play in the maritime industry", said South. The first is automation itself, as machinery on vessels is increasingly controlled by software. The second is integration. On any given vessel, there may be multiple systems connected together. The third is the ability of ship-to-shore systems that communicate via remote monitoring. "Ships are now talking to head offices continuously," says South. The fourth factor is that all these systems are connected through the internet.

All these factors apply to harbours and maritime infrastructure as well and must be considered.

Myanmar: The Situation

In Myanmar, we should consider the actual situation, which has been presented during a Capacity Building Workshop on Strengthening Transport Connectivity among CLMV-T, 9-10 October 2018, Yangon, Myanmar.

Myanmar´s total coastline is 2,228 km, the continental shelf 228,000 km and territorial waters 486,000 km, including the EEZ. Myanmar also possesses the five major rivers for inland water transport:

1. Ayeyarwady River,
2. Chindwin River,
3. Thanlwin River,
4. Sittaung River and
5. Kalardan River.

The total length of these rivers is approx. 8,000 miles, navigable waterways about 2,000 miles with more than 400 river ports. Myanmar has a total of nine ports catering mainly for its seaborne and coastal trade spread over the whole coastline Yangon is the main port city of Myanmar (and former capital city).

Part one: Protection of Harbours

The protection of harbours against hybrid threats is an ongoing task for all civilian harbours, be they sea ports or river ports and naval bases. They constitute a vital part of the whole logistic chain for goods, and they are also resources for navies and military transport. Harbours are part of the global critical maritime infrastructure and they constitute the gateway between sea and land.

Protection, like security and resilience, is a multi-faceted term, particularly in a maritime context. Traditionally, to the military it implies the allocation of men and equipment to specific tasks in response to threat intelligence by active surveillance, detection and monitoring of the environs and defensive perimeter measures. Civilians have been more likely to adopt a risk-based approach taking account of their responsibilities and authorities as limited by law, geography and ownership. As hybrid threats pose a combination of threats, risks and challenges, that are neither purely military nor civilian, they require an integrated response spanning both approaches. Workshops to gather and share views between civilian and military – two communities which have rare opportunities to meet, but which hybrid threats require to meet more often.

Part two: Maritime Trade

The maritime trade world is multi-dimensional with many stakeholders and few clear boundaries. It is the backbone of globalization facilitating long, complex supply chains through fragmented regulatory frameworks. It is also highly competitive and thus reluctant to absorb additional costs. Individual or associations of stakeholders are limited in their ability to enforce security standards outside their own particular place in the supply chain, thus opening opportunities for risk arbitrage by hostile or criminal groups. Shipping companies and harbour authorities have responded by developing sophisticated communication and intelligence networks to facilitate their understanding of routine markets and risks. But commercial

entities have a finite capacity and limited resources and can be overwhelmed by terrorism, cyber-attacks, environmental challenges, financial, social or other catastrophic events beyond their control. In a crisis situation when the limits of resilience have been reached external assistance may be required to withstand further threats or to enable recovery.

Part three: Definition of Hybrid Warfare

Definition of hybrid warfare
Hybrid warfare is essentially asymmetric in its way of taking action exploiting such differences, attacking vulnerabilities and weaknesses rather than fortresses. Weaknesses in this context must be understood as the absence of a coordinated plan between civilian and military authorities and the lack of common vulnerability assessments.

Countering hybrid threats requires an agreed definition or at least a common understanding between all actors responsible for protecting harbours against this threat. Several attempts have been made at defining a complex and cross-cutting concept:

"*While definitions of hybrid threats vary and need to remain flexible to respond to their evolving nature, the concept aims to capture the mixture of coercive and subversive activity, conventional and unconventional methods (i.e. diplomatic, military, economic, technological), which can be used in a coordinated manner by state or non-state actors to achieve specific objectives while remaining below the threshold of formally declared warfare. There is usually an emphasis on exploiting the vulnerabilities of the target and on generating ambiguity to hinder decision-making processes. Massive disinformation campaigns, using social media to control the political narrative or to radicalize, recruit and direct proxy actors can be vehicles for hybrid threats*."[10]

"*The fundamental idea of hybrid-warfare is to find the space short of clear-cut military action with direct and recognizable tactical, operational, and strategic impact and compress it into a zone where insufficient ambiguity is created to allow an offensive actor a better chance of accomplishing an objective without fullblown, overt offensive action*."[11]

Finally, in this list of attempts, the document "Understanding Hybrid Warfare" includes a very concise definition of hybrid warfare (because of lack of consensus it is presented as a description, but formally it is a definition): "*The synchronized use of multiple instruments of power tailored to specific vulnerabilities across the full spectrum of societal functions to achieve synergistic effects.*"[12]

While none of them has reached universal acceptance, the combination of these three attempted definitions encapsulates the concept very well and demonstrates the civilian and military components of the challenge posed.

The diversity of options available to an invader are manifold and to safeguard ships, harbours, anchorages and maritime infrastructure as a whole must be understood as requiring a comprehensive approach, involving all maritime services and governmental and private authorities.

"To safeguard harbours and ships from cyber threats, companies should follow International Maritime Organization approved guidelines on cyber risk management, which focus on identifying the systems, data and capabilities that pose a risk to operations, when they are disrupted. To do that, companies must implement risk control processes and have the ability to detect cyber events in a timely manner. They must also be able to back-up and restore systems necessary for shipping operations or services impaired following a cyber event."

Part four: General Setting

Seaports are generally built near or inside a town, or alongside a river and are connected to the hinterland by road and rail. There are often no continuous walls to separate the port area from the town, only particular critical installations are protected. With ports open to the town and sensitive locations not far from built up areas, the surroundings of the port area must be under surveillance.

Every day, thousands of people go to work inside the port area, hundreds of cars and trucks have to enter and leave, numerous industrial sites or terminals operate within the area, thousands of passengers have to transit through and maritime traffic is permanently moving on the water or alongside the quays.

Different aspects have to be considered in order to achieve a better and real awareness of the situation.

The challenge are increased security requirements and the harbour manager has to consider: how to optimize the movement of cargo—ensuring that containers, personnel, ships, trucks, and rail traffic move in and out of port as efficiently as possible.

What could be done:

Maximize the mobility and productivity of personnel by enabling them to access data and communicate with each other from any point in the facility.

Monitor security throughout the port by screening the port and its perimeter, as well as containers, ships, trucks, rail, cars and personnel that enter or leave the facility.

Comply with government regulations. Monitor security throughout the port. Unify and upgrade the facility's communication systems for greater operational efficiency.

The following text is a modified quotation from „Countering Hybrid Threats in the Maritime Environment":

[10] Quotation from the Joint Communication to the European Parliament and the Council, April 2016

[11] ADM Stavridis in the Proceedings of the US Naval Institute, 2016

[12] Multinational Capability Development Campaign "Understanding Hybrid Warfare" January 2017

Commercial aspects

Vessels of all kind and sea and river ports, are vulnerable to hybrid threats.

Sabotage, navigational spoofing, and cyber-attacks on supply chain information systems. At the same time, foreign ownership and control of commercial port facilities can lead to the disruption of their use when these same facilities are required in times of crisis. This is already a major concern.

Cyber aspects

Commercial and military maritime activities are more reliant on cyber-enabling capabilities than ever, with everything from navigation systems to port information systems all being vulnerable to cyber-attack by hybrid actors and criminal organizations. The Maersk incident of 2017 illustrates the challenge well. A cyber-attack on the government of Ukraine inadvertently impacted Danish global shipping giant Maersk when they went to pay their Ukrainian taxes online.

As a result, Maersk's global operations came to a halt as they temporarily lost the ability to govern their fleet. Numerous other industries were also impacted as the global supply chain was disrupted.5 If this attack was actually aimed at commercial ports and logistics companies, the damage and disruption could have been much worse.

Information held by a port such as the financial and business transactions of its many stakeholders, attracts cyber-attackers to target ports and port facilities whose computer systems and databases may include the control of safety infrastructure such as pumps, storm and flood barrages.

As a general rule, while individual ports are important, the number of ports and competition provides redundancy. Practical experience has proven that common sense and practical measures are required as well as sophisticated solutions. The central role of the State in protecting harbours is obvious, but the capabilities used to enforce protection vary widely due to geography, function, culture and tradition creating a complex environment for enforcing protection.

Cyberattack is a key element in current hybrid attacks, occurring in almost all spheres of life on a daily basis. Cyberattacks are disrupting digital services in harbours, reducing the effectiveness of logistic chains and personnel security. There is a need to discuss how to improve the resilience of communication and information systems. Cyber threats to maritime security have been addressed in the EU Maritime Security Strategy and its Action Plan. The threats caused by manned and unmanned systems, in all three dimensions, air, surface and subsurface must also be assessed. These systems have a cyber dimension that could be exploited to cause physical and organizational damage. Cyber threats are a growing menace, spreading to all sectors of industry that progressively rely on Information and Communication Technology (ICT) systems. Recent examples of deliberate disruption of critical automation systems prove that cyber-attacks can have a significant impact on critical infrastructure. Disruption or unavailability of these ICT capabilities may have disastrous consequences for all governments and social stability. The need to ensure reliability and ICT's robustness against cyber-attacks is thus a key challenge at national and international level.

Critical information infrastructure supports vital services and goods such as energy, transport, telecommunications, financial services, etc., that are so essential that their unavailability may adversely affect the well-being of a nation. Maritime transport is no exception. Whether it is the logistics chain or the ships themselves, global maritime trade can no longer ignore this risk. Navigation systems, telecommunications, energy management systems, and possible entry points must not only be considered upstream, during the design of ships and harbour control systems, but also subsequently as electronic and computer systems need to be updated continuously to meet emergent risks.

Due to their significant importance, the protection of critical information infrastructure is required to sustain and further enhance the well-being of societies, the global and national economy. The subject has therefore drawn the attention of the policy makers in national governments and regional and global fora.

Energy aspects

Diversification of energy supplies has led to an increase in the importance of liquefied natural gas (LNG), to include the transport vessels and onshore offloading facilities. In addition, gas and oil exploration in many maritime domains and the trans-shipment of petroleum and LNG at sea makes the energy supply chain more vulnerable to hybrid threats against the commercial entities which explore, extract, and ship these commodities.

Communications aspects

Today's economies are very reliant on the global information technology infrastructure with 97 percent of intercontinental communications moving through undersea cables, most of which lack even basic defences. These cables are not owned by states, but rather by private entities which cannot afford to harden them and still make a profit.

The potential impacts are apparent when considering that in December 2008, accidental cable cutting in the Mediterranean and Persian Gulf resulted in widespread internet outages in the Middle East and India.

Territorial Vulnerability aspects

The borders and exclusive economic zones (EEZ) of coastal nations can be disrupted and contested by hybrid actors acting on behalf of a state in order to contest the governance of their sovereign territory. In the South China Sea, China seeks to expand its claims, often interfering with the territorial waters and exclusive economic zones (EEZ) of countries like Vietnam and the Philippines, using methods such as

armed fishermen to challenge the authorities of these nations and their commercial entities operating in their own EEZ.

Since the ability to control, maintain, and protect sovereign territory is a key aspect of governance, these are among the central tasks of coast guards and naval forces. In some cases, governments find it necessary to modify the rules of engagement for coast guards to be authorized to use deadly force, as Finland did in 2017.

Maritime Security Forces aspects
Clandestine hybrid actors using armed frogmen or unmarked vessels disguised as commercial or fishing craft can surprise and swarm military vessels, disabling or disrupting them to keep them from being able to respond to other elements of a hybrid attack. The ability to detect, attribute, and respond to these threats is among the greatest challenges presented to security forces. In addition, the availability of increasingly sophisticated commercial off-the-shelf technology (COTS) to hybrid actors means that maritime security forces must constantly adapt in order to mitigate these emerging risks.

Disinformation aspects
Alongside the previously mentioned maritime hybrid threats is the vulnerability to adversary disinformation campaigns aimed at eroding internal and regional trust by creating a false counter narrative. These disinformation campaigns across the media spectrum can bring into question the intentions and activities of friendly maritime security forces and their governments, not just in other countries but at home among their own people.

Military and civilian aspects
When talking about the necessity to improve the awareness for these vulnerabilities, risks and threats it became very obvious that there is a gap between civilian and military threat assessments and a notable lack of common understanding in thinking, planning and acting. How far this lack of common understanding and planning is relevant for the development of common capabilities deserves further investigation but depends on the willingness of all stakeholders to come together in an open and transparent way. The special role of Naval Bases and Stations and how far their security measures and experiences can be of general value is relevant for protection against hybrid threats to civilian harbours, depending on the country concerned.

Conclusions

Hybrid risks and threats are more than cyber, but cyber offers the best and a most efficient option for an attack which does not need people on the ground and which is difficult to detect. Sometimes it will never be discovered. For a long time, governmental and private stakeholders assessed cyber as purely an information technology issue and were the responsibility of the IT department. There is no doubt that a technical knowledge is essential but the technical aspect is only one of several other aspects and the best way to approach the situation is by a comprehensive approach. People who are responsible for security must have an understanding of all three levels of possible impacts: the strategic level, the operational and management level and the tactical level which means people on the ground. And all experience indicates that people are the weakest link in the chain of all security plans. People on all three levels could be targets, but the people on the ground could easily be hacked when using the Information technology to do their job efficiently and professionally. Cyber security is a leadership responsibility and people at all levels have a responsibility to share concerns and anomalies with their superiors who must have a direct access to the leadership/management people whether in government organisations or private companies.

The aspect of “good governance” is closely linked with the demand for better and deeper coordination and cooperation between the public and the private sectors. Good governance is also based on international cooperation when it comes to finding appropriate solutions and coordinating actions against hybrid attacks and specific cyber threats.

A whole-of-government approach is required in which all agencies and ministries from national to local level cooperate and share information to reduce any gaps, seams, and vulnerabilities which can be exploited by hybrid and transnational threats.

A whole-of-society approach is needed, which is similar to the whole-of-government approach, but also includes engagement with the private sector, academia, and civil society stakeholders.

Placing the focus on governance, instead of looking at hybrid and transnational threats primarily through a military lens, does not exclude a role for military capabilities.

Naval stations have their own security standards which are based on national rules. They have their internal alert systems which do not necessarily correspond with the standards of civilian ports. These alert systems are based on a broader security assessment which takes the hinterland of a Naval Station into consideration as well.

The European Union´s and NATO´s harbour protection activities for example, are based on four principles: they are multinational, deployable, modular and executed on the “plug and play” principle. The task includes protecting ships at anchor/berths as well as port infrastructure in expeditionary operations where host nation’s harbour protection capabilities are limited or non-existent. The activities should provide deployable harbour-protection against tri-dimensional threats and integrate/execute Command and Control functions.

Rather, it puts military capabilities into a perspective which more closely matches each nation’s own legal authorities and frameworks. Given the nature of these threats, the first to detect and respond are most likely to be civilian entities (both public and private),

which may nevertheless require varying degrees of military capabilities to provide support. This is especially important since no government can afford to provide different sets of capabilities and this would undermine the responsibility to share information and knowledge. If risks become threats close civil-military cooperation is vital and this includes interoperability. This is another argument for "dual use" capabilities to counter hybrid and cyber threats.

Cyber-attacks are reported to the national cybersecurity agencies in the countries where they exist. Tools could be developed to facilitate and accelerate information exchange between the appropriate communities (port authorities, ship-owners, companies, military commands).

Only a comprehensive range of sensors operating in different environmental domains, with the information they provide being collated and processed in real time, can provide a reliable picture of the situation. Vulnerable single sensors like AIS should be only one of several sources of information.

Unmanned systems are a future core element of harbour's security systems, especially for very long-lasting, monotonous activities for persistent monitoring of the harbour waters or providing means of identification/classification and countermeasures.

New technologies (Artificial Intelligence, swarm intelligence,) can be used to counter threats. Resilience of systems should be very carefully studied and updated with technological progress. Weaknesses should be addressed. Capabilities to interfere with system functions are constantly increasing. In this field, artificial intelligence plays a very important role and a very interesting idea – swarm intelligence – that can and must be used in autonomous systems.

The lack of coordination between stakeholders in information exchange and coordination between national and international agencies creates major discrepancies in tackling maritime security risks and threats. It would be helpful if governments could provide a lead in developing a platform for further consultation and coordination on maritime cyber security. The European Union has established two Centres of Excellence dealing with cyber risks and threats.

A last but not least aspect should be mentioned. Training and exercises are crucial in any kind of security and defence related activity, but even more so in countering hybrid warfare, where recognising the existence of an attack from a set of apparently random events is a particular difficulty faced by those responsible. Frequent table top and communications exercises presenting scenarios as variable as the imagination can go are vital. These exercises must involve all three levels, strategic, operational and tactical very importantly, port authorities and harbours security directors.

Lutz Feldt

Vice Admiral (rtd) Feldt served in the German Navy for 41 years and retired in 2006 as Chief of the German Naval Staff in Bonn and Berlin. He was engaged in sea duty assignments for 13 years, which included leadership functions on all command levels and duty assignments in different naval staffs, national and in NATO.
Since retirement, he has occupied several posts of honor. Vice Admiral Feldt was president of the German Maritime Institute until June 2012 and is now a member of its board. From 2008 until 2009 he was working for the European Commission as advisor for the "Instrument for Stability". From July 2009 to December 2010 he served the European Defence Agency as member of the Wise Pen Team, working on topics of maritime surveillance and maritime security. From November 2013 until March 2017 Vice Admiral Feldt was President of EuroDefense Deutschland e.V.
Since August 2011, Vice Admiral Feldt, in his function as a Director of the Wise Pens International, is working on studies dealing with future maritime safety, security and defence, for example "On the Future of EU Maritime Operations Requirements and planned Capabilities" together with his fellow Directors. Recently they have finalized a study about "Naval Challenges in the Arctic Region".
This paper was presented at the joint conference Security Threats in the 21st Century of the Myanmar Institute of Strategic and International Studies (MISIS) and the Konrad Adenauer Foundation (KAS) on November 26, 2018 in Yangon, Myanmar.
It was first published in ISPSW Strategy Series: Focus on Defense and International Security, Issue No. 596, January 2019.
www.ispsw.de
Opinions expressed in this contribution are those of the author.

References

References used and benefitted from:
1. Hybrid Warfare Protection of Harbours, A report by Wise Pens International, June 2018, not published
2. MCDC Understanding Hybrid Warfare, January 2017
3. Cyber security in the maritime industry www.mondaq.com/canada/x/667590/Marine+Shipping/Cybersecurity+In+The+Maritime+Industry
4. Joint Communication to the European Parliament and the Council, April 2016 www.eumonitor.nl/9353000/1/j9vvik7m1c3gyxp/vkhn74f29mz1
5. Hybrid threats in the maritime environment http://cimsec.org/countering-hybrid-threats-in-the-maritime-environment/36553
6. Maritime Hybrid Warfare Is Coming by ADM James Stavridis www.usni.org/magazines/proceedings/2016-12-0/maritime-hybrid-warfare-coming

IMPRESSUM

Denk*würdigkeiten*
Journal der
Politisch-Militärischen
Gesellschaft e.V.

Herausgeber
Der Vorstand der **pmg**

Redaktion
Ralph Thiele (V.i.S.d.P.)
E-Mail: info@pmg-ev.com
Webseite: www.pmg-ev.com

Die **Denk*würdigkeiten*** erscheinen mehrfach jährlich nach den Veranstaltungen der **pmg**.