Zeitenwende braucht Mentalitätswandel

Die Welt ist unsicherer geworden – und Europa muss sich darauf einstellen. Beim Fachforum Zukunft.DEFENCE diskutierten Experten, welche Rolle die zivile Wirtschaft beim Aufbau von Verteidigungsfähigkeit spielen kann.

VON JÜRGEN GROSCHE

Das Interesse an der zweiten Fachkonferenz Zukunft.DEFENCE war groß. Zahlreiche Besucher informierten sich im Konferenzzentrum der Rheinischen Post in Düsseldorf über Geschäftsmöglichkeiten im Verteidigungssektor und nutzten die Veranstaltung zum Netzwerken. FOTOS: VOGT GMBH

Die Entwicklung der vergangenen Jahre, insbesondere der Ukrainekrieg, haben das Thema Verteidigung wieder ganz nach oben auf der politischen und gesellschaftlichen Agenda gerückt. Viel ist von „Zeitenwende“ die Rede. Staaten, Wirtschaft und Gesellschaft investieren viel in den Aufbau einer stärkeren Verteidigungsfähigkeit. Gefragt sind hier auch die Entwicklungs- und Produktionskapazitäten der zivilen Industrie sowie dere Fähigkeit zur schnellen Skalierung.

Wie können zivile Industrie, die OEMs (Original Equipment Manufacturer bzw. Originalausrüster) der Sicherheits- und Verteidigungsindustrie und die Bundeswehr als Beschaffer in den direkten Dialog kommen? Darum ging es im Juni bei der zweiten Fachkonferenz Zukunft. DEFENCE im Konferenzzentrum der Rheinischen Post in Düsseldorf. Die Veranstalter Rheinische Post sowie griephan by DVV Media und der publish-industry Verlag hatten sich gemeinsam mit dem ZVEI (Verband der Elektro- und Digitalindustrie) die Ziele gesetzt, Bedarfe, Beschaffungswege und Rahmenbedingungen transparent zu machen und realistische Geschäftspotenziale sowie Grenzen aufzuzeigen und darüber hinaus Partnerschaften zu fördern. Die erste Veranstaltung im Dezember war bereits sehr erfolgreich und zeigte den Bedarf an Austausch und Information.

In kleinen Gruppen vertieften die Teilnehmer einzelne Themenbereiche.

„Defence ist ein Thema, das uns alle umtreibt.“ Mit diesen Worten eröffnete Kilian Müller, Geschäftsführer des publish-industry Verlages, die Fachkonferenz. Bernhard Müller-Härlin vom ZVEI ergänzte: „Der Aufbau von Verteidigungsfähigkeit ist keine Aufgabe einzelner Branchen – er ist eine gesamtindustrielle Gemeinschaftsaufgabe.“ Moderne Verteidigungssysteme basierten zunehmend auf Elektronik und Software; gefragt sei die gesamte Wertschöpfungskette, nicht nur die klassischen Rüstungsunternehmen. Den inhaltlichen Auftakt bestritt Prof. Dr. Stefan Fröhlich, Experte für internationale Politik und politische Ökonomie, mit einer nüchternen Analyse der Weltlage. Seine Kernthese: Die Zeitenwende habe nicht erst mit dem russischen Einmarsch in die Ukraine 2022 begonnen. „Sie fand längst statt. Das wird immer noch verdrängt.“ Fröhlich skizzierte drei Trends, die das weltpolitische Geschehen bestimmten.

Erstens: die Rückkehr der Geopolitik. Der Krieg ist auf den europäischen Kontinent zurückgekehrt – was lange als überwunden galt, ist bittere Realität. Zweitens eine geoökonomische Verschiebung, die spätestens mit der Weltfinanzkrise 2007/2008 begann. Bis zur Jahrtausendwende generierten die klassischen OECD-Länder noch rund 75 Prozent der weltweiten Wirtschaftsleistung, heute sind es knapp 50 Prozent. Der Aufstieg Chinas und der Schwellenländer hinterlässt Spuren. Billige Energie aus Russland, günstige Produktion und ein scheinbar endloser Absatzmarkt in China sowie von den USA garantierte Sicherheit – diese gewohnten Vorteile sind zerstört, ökonomische Instrumente werden zu politischen Waffen. Drittens der Systemwettbewerb zwischen Autokratie und Demokratie: China strebe eine neue Weltordnung an, die westliche Hegemonie solle gebrochen werden. Diese Gemengelage befördere Protektionismus, Nationalismus und Rechtspopulismus – in elf von 27 EU-Staaten ist heute eine rechtspopulistische Partei an der Regierung beteiligt.

Was folgt daraus? Europa müsse strategische Autonomie zurückgewinnen, ohne sich abzuschotten – eine Gratwanderung. „Wir müssen in den Bereichen Wirtschaft, Handel und Sicherheit autonomer werden“, sagte Fröhlich. Vollständige Autarkie sei unrealistisch, wohl aber ein gezieltes De-Risking – die Verringerung gefährlicher Abhängigkeiten. Voraussetzung: Europa müsse mit einer Stimme sprechen.

Für das Thema Verteidigung wurde Fröhlich besonders konkret. Die Erhöhung der Verteidigungsausgaben sei „keine Frage des Geldes, sondern der Umsetzung“. Genau hier lägen die größten Probleme – wie das Scheitern des FCAS-Projekts zeige, eines gemeinsamen deutsch-französischen Programms zur Entwicklung eines Kampfflugzeugsystems der nächsten Generation. Eine EU-Armee werde es nicht geben, denkbar seien aber „Koalitionen der Handlungswilligen“, wie sie sich zwischen Frankreich, Großbritannien, Polen und Deutschland bereits abzeichneten. Europa müsse so handeln, als stehe Amerika nicht mehr automatisch an seiner Seite – und im eigenen Umfeld die konventionelle Verteidigung selbst übernehmen.

Fröhlich diagnostizierte eine erhebliche „Fähigkeitslücke“: Auf absehbare Zeit bleibe Europa auf Rüstungsgüter aus den USA angewiesen, müsse aber parallel die eigene Industrie stärken. Hier kommt die zivile Wirtschaft ins Spiel – der ZVEI hat dafür eigens die Plattform „Sicherheit und Verteidigung“ ins Leben gerufen, um Unternehmen beim Einstieg in diesen anspruchsvollen Markt zu begleiten.

Doch am Ende, so Fröhlich, sei es eine Frage, die weit über Haushaltszahlen hinausgehe: „Wir brauchen einen Mentalitätswandel.“ Die Debatten über die Wiedereinführung der Wehrpflicht zeigten, dass viele die Tragweite der Lage noch nicht begriffen hätten. Die Zeitenwende sei kein Ereignis – sie sei ein Prozess. Und Europa stehe mittendrin.

Ukraine als härteste Qualitätsprüfung der Welt

Spannend war der Einblick in die ukrainische Beschaffungspolitik, den Mattia Nelles vom Deutsch-Ukrainischen Büro gewährte.

Die Ukraine sei ein „Realitätscheck für europäische Defence-Produkte“, lautete die Kernthese des Ukraine-Kenners – schließlich müssen sich alle Systeme unmittelbar im Kampfgeschehen bewähren. Die Lage sieht nach Nelles’ Darstellung derzeit so aus: An der Front gibt es keine klaren Linien, sondern eine „graue Zone“ von 25 bis 30 Kilometern Tiefe, in der jedes sichtbare Ziel bedroht wird. Unbemannte Drohnen und Landfahrzeuge haben in diesem Umfeld enorm an Bedeutung gewonnen.

Unter diesem immensen Druck hat die Ukraine nach Nelles‘ Darstellung den schnellsten Rüstungs-Innovationszyklus der Welt geschaffen: Statt der sonst üblichen Jahre dauert er nur noch zwei bis sechs Wochen. Sechs neue Waffensysteme werden täglich zertifiziert, für dieses Jahr sind sieben Millionen Drohnen geplant. 90 Prozent dieser unbemannten Systeme sollen aus ukrainischer Eigenproduktion kommen.

Vor diesem Hintergrund gewinnt die Definition „kampferprobt“ (battle-proven) als Qualitätsmerkmal für Rüstungsgüter eine andere Bedeutung. Während in Friedenszeiten dafür Tests auf einem Übungsgelände und eine NATO-Zertifizierung reichen, lassen die Ukrainer nur gelten, was russische Angriffe überlebt hat. Da der Gegner ja auch dazulernt, müssen die Produkte schnell angepasst werden.

Für Unternehmen, die in diesem Markt Fuß fassen wollen, nennt Nelles klare Voraussetzungen: Präsenz vor Ort in Kiew, funktionierende Reparatur- und Ersatzteilstrukturen im Land sowie wöchentliche Rückmeldungs- und Anpassungszyklen direkt aus dem Einsatz.

Wer in der Ukraine in der Rüstungsbranche Geschäfte machen will, muss gut sein und schnell, erklärte Mattia Nelles, Geschäftsführer des Deutsch-Ukrainischen Büros. FOTO: VOGT GMBH

Sein Rat an die Industrie fällt pointiert aus: „Die Ukraine ist nicht euer Markt. Sie ist eure Forschungs- und Entwicklungsabteilung.“ **jgr**

INFO

Veranstaltungen, die verbinden und informieren – das ist auch das Ziel des RP Forums, der Dialog- und Veranstaltungsplattform der Rheinischen Post.
Mehr im Internet:
www.rp-forum.de

Ein Markt für viele Branchen

Die militärische Zeitenwende ist längst kein Thema mehr allein für klassische Rüstungsunternehmen – auch Branchen wie Schienenfahrzeugbau und Elektronikindustrie entdecken den Verteidigungsmarkt für sich.

VON JÜRGEN GROSCHE

Neben Einzelvorträgen gab es auch Fachdiskussionen zu Themen rund um Defence. FOTO: VOGT GMBH

Beim Fachforum Zukunft. DEFENCE stellten mehrere Unternehmen aus unterschiedlichen Segmenten ihre Erfahrungen beim Eintritt in den Verteidigungsmarkt vor, unter anderem der Schweizer Hersteller von Schienenfahrzeugen Stadler Rail. Eisenbahn und Militär – ein klassisches Beispiel für Dual-Use, also Güter, die sowohl zivil als auch militärisch genutzt werden können. „Was können wir mit unseren Stammprodukten tun, um militärische Mobilität sicherzustellen?“, fragte Catharina Dohmeier, Verkaufsleiterin Dual Use & Spezialfahrzeuge bei Stadler Rail, und brachte damit das Kernthema auf den Punkt.

Unternehmen, die sich für die Weiterentwicklung ihrer Produkte für die Verteidigung interessieren, sollten zunächst ihre Kernkompetenzen klären, das politische Marktumfeld analysieren und schauen, wie die Kernkompetenzen zur Umfeldentwicklung passen. Konkret fragte man sich bei Stadler, wie militärische Mobilität ausgestaltet sein muss und welchen Beitrag man leisten könne. Eine kleine Anfrage im Bundestag hatte offenbart, dass das gesamte Schienennetz in Deutschland grundsätzlich auch für die Verteidigung nutzbar sei. Stadler brachte sich mit dem Argument ins Spiel, mit seinen Fahrzeugen konkret zur Verteidigungsbereitschaft beitragen zu können, insbesondere mit einem Fokus auf Vorsorgethemen.

Udo Hoffmann von Schneider Electric, einem französischen Elektrotechnik-Konzern mit Fokus auf Produkten für die Automatisierung, Energieverteilung und Installationstechnik, konnte ebenfalls aus dem Kerngeschäft die Relevanz auch für den Verteidigungssektor darstellen. Das Unternehmen liefert integrierte Komplettlösungen für Gebäude, Rechenzentren und kritische Infrastrukturen wie Energieversorger oder Krankenhäuser – also genau jene Anlagen, deren Versorgungssicherheit im Verteidigungsfall besonders zählt.

Was im zivilen Bereich längst Standard ist – vernetzte Energie-, Wärme- und Mobilitätslösungen etwa in Wohnquartieren –, lässt sich direkt auf militärische Liegenschaften übertragen. Hoffmann nannte als konkretes Beispiel Bundeswehr-Immobilien und Luftwaffenstützpunkte: Auch dort brauche es zuverlässige Energieversorgung und autarke Microgrid-Systeme, die im Krisenfall unabhängig vom öffentlichen Netz funktionieren. Zum Geschäft von Schneider Electric gehört, so die Botschaft, auch die Verteidigung – ohne dass das Unternehmen je ein Waffensystem gebaut hat.

Die Verteidigungsindustrie bietet auch Mittelständlern Perspektiven, wie Jan Horn vom Unternehmen Instagrid aus Ludwigsburg berichtete. Der Hersteller leistungsstarker mobiler Stromspeicher bietet seine Produkte auch für die Verteidigung an. Die Batteriesysteme von Instagrid wurden von der Wehrtechnischen Dienststelle für landgebundene Fahrzeugsysteme (WTD 41) der Bundeswehr erfolgreich im Praxiseinsatz getestet und für die mobile, geräuschlose und emissionsfreie Energieversorgung genutzt.

Möglichkeiten zur Geschäftsentwicklung im Rahmen der Ukraine-Unterstützung stellte schließlich Oberstleutnant Christian Hohoff vom Sonderstab Ukraine im Bundesverteidigungsministerium vor. In der Ukraine seien ausländische Unternehmen sehr willkommen und würden vom Militär unterstützt. Firmen, die dort Erfolg hätten, seien auch in anderen Ländern geschätzt.

Doch Hindernisse ganz anderer Art dürften nicht aus dem Blick geraten, mahnte Prof. Dr. Thomas Klindt, Senior Partner bei der Kanzlei Noerr: Die regulatorischen Rahmenbedingungen für die zivile Industrie im Defence-Markt seien „strenger als in der Medizintechnik“. Unternehmen sollten sich davon nicht abschrecken lassen. „Sie stehen zunächst vor verschlossenen Türen. Dahinter öffnen sich tolle Landschaften.“

Das Regelwerk ist ziemlich umfassend und reicht vom Exportkontrollrecht mit Genehmigungspflichten über Investitionsprüfungen bis zum Sanktionsrecht. „Fehltritte werden sofort gnadenlos juristisch verfolgt“, warnte der Rechtsexperte, der empfiehlt, den Rat von Juristen einzuholen. „Sie helfen, die Minen aus dem Weg zu räumen. Man muss wissen, wo diese Minen liegen.“

Cybersecurity muss Chefsache sein

Neun von zehn deutschen Unternehmen glauben, gut gegen Cyberangriffe gerüstet zu sein. Sicherheitsexperte Wolfgang Straßer widerspricht vehement – und warnt vor blinden Flecken mit Milliardenschäden. Besonders im Visier von Angreifern: die Defence-Branche.

VON JÜRGEN GROSCHE

Wolfgang Straßer, Geschäftsführender Gesellschafter der @-yet GmbH FOTO: WOLF BUSCH

Wolfgang Straßer gehört zu den Mahnern, die oft überhört werden. Der Cybersecurity-Spezialist und Geschäftsführender Gesellschafter der @-yet GmbH weiß, wovon er spricht, wenn er sagt: „In einem zunehmend volatilen geopolitischen Umfeld gehört CyberSecurity eigentlich auf die Agenda der Führungskräfte – und muss strategisch und ganzheitlich angegangen werden.“ Die Betonung müsste auf dem Wort „eigentlich“ liegen, denn die Realität sieht trotz aller Mahnungen anders aus.

Straßer zitierte bei der Fachkonferenz Zukunft.DEFENCE Zahlen aus der „TÜV Cybersecurity Studie 2025“, nach denen 91 Prozent der befragten deutschen Unternehmen ihr Cybersicherheitsniveau als „sehr gut“ oder „gut“ bewerten. Mit ihrem Eigenbild liegen sie indes „krass daneben“, kommentierte der Sicherheitsexperte die Ergebnisse. Das eigene Cybersicherheitsniveau werde drastisch überschätzt, wie steigende Angriffszahlen und wachsende Schäden zeigten.

Mit mehr als 90 Mitarbeitern berät das inhabergeführte Leichlinger Unternehmen seit 24 Jahren Mittelständler, Konzerne und Organisationen unterschiedlichster Art – in Deutschland und weltweit. Viele kommen zu den Sicherheitsexperten erst, wenn der Schaden da ist. „Jeden Tag sind wir mit Vorfällen beschäftigt“, berichtete Straßer. Die Angriffe reichen von Erpressung und Finanzbetrug über Spionage und Infiltration, Manipulation und Desinformation bis hin zu physischer Sabotage. Allein im vergangenen Jahr entstanden in Deutschland Schäden durch Cyberangriffe in Höhe von 290 Milliarden Euro. „Das sind 4,7 Prozent der deutschen Wirtschaftsleistung“, ordnete Straßer die Zahlen ein.

Natürlich steht der Defence-Sektor ganz oben auf der Speisekarte der Angreifer – geht es doch nicht nur um wirtschaftliche Aspekte, sondern um globale Sicherheitsthemen. „Attacken aus China, Russland, dem Iran und aus Nordkorea destabilisieren unsere Gesellschaft planvoll und mit ganzheitlichen Attacken-Strategien“, warnte der Experte. In Europa sei dies noch nicht so ins Bewusstsein gedrungen wie in den noch stärker bedrohten Ländern Ukraine und Israel.

Unternehmen müssen sich verstärkt mit Sicherheitsthemen befassen. Das gilt generell, besonders aber im Defence-Sektor. FOTO: GETTYIMAGES/SOLARSEVEN

Unternehmen müssen sich, so Straßer, verstärkt mit Sicherheitsthemen befassen. Das sei Grundvoraussetzung, wenn sie in diesen Ländern geschäftliche Kontakte knüpfen wollen. „Man muss zum Beispiel auch darauf achten, dass die Lieferketten besser geschützt werden. Die NIS 2.0 trägt dem Rechnung, muss jetzt aber auch konsequent von den betroffenen Unternehmen umgesetzt werden.“ (Die NIS-2-Richtlinie ist der europäische Standard für Cybersicherheit.) Daher seine Forderung: „Das Thema gehört ganz oben auf die Agenda der Führungskräfte und erfordert einen ganzheitlichen Ansatz.“

Ein solcher Cybersecurity-Ansatz umfasse etwa Steuerung und Vorbereitung, technische Prävention sowie Vorfallsbewältigung. Dazu gehören zum Beispiel Sicherheitslückenanalysen, Informationssicherheits-Managementsysteme, Schulungen, Penetrationstests, Krisenbereitschaft, Erkennung, Forensik und Wiederaufbau. „Wenn etwas passiert, sollte man vorbereitet sein“, forderte Straßer. „Das sind aber die meisten Unternehmen nicht.“ Es gebe im Management immer noch kein ausreichendes Bewusstsein für die Dringlichkeit. IT-Leitung und Admins seien nicht ausreichend ausgebildet, und IT-Systemhäuser seien bei Infrastruktur und IT-Sicherheit eher nicht gut aufgestellt.

Speziell für den Defence-Bereich nannte Straßer weitere Anforderungen: Mindestens ein Grundschutz nach ISO 27001 oder BSI-Standards (des Bundesamts für Sicherheit in der Informationstechnik) müssen vorhanden sein; in VS-NfD-Umgebungen (Verschlusssache – Nur für den Dienstgebrauch) sei eine nachgewiesene Geheimschutzfähigkeit erforderlich. Zu schützen seien insbesondere Forschung und Entwicklung, Geschäftsstrategien sowie Personalberechtigungskonzepte (Wer darf auf was zugreifen?). Netze müssten segmentiert, Daten verschlüsselt werden; klare Regeln für Zugangskontrollen und Social-Media-Nutzung seien ebenso unerlässlich wie Personalüberprüfung und Compliance. Klingt anspruchsvoll – aber wer gute Geschäfte machen und keine schweren Schäden erleiden will, kommt da nicht drum herum.

Internet: www.at-yet.de