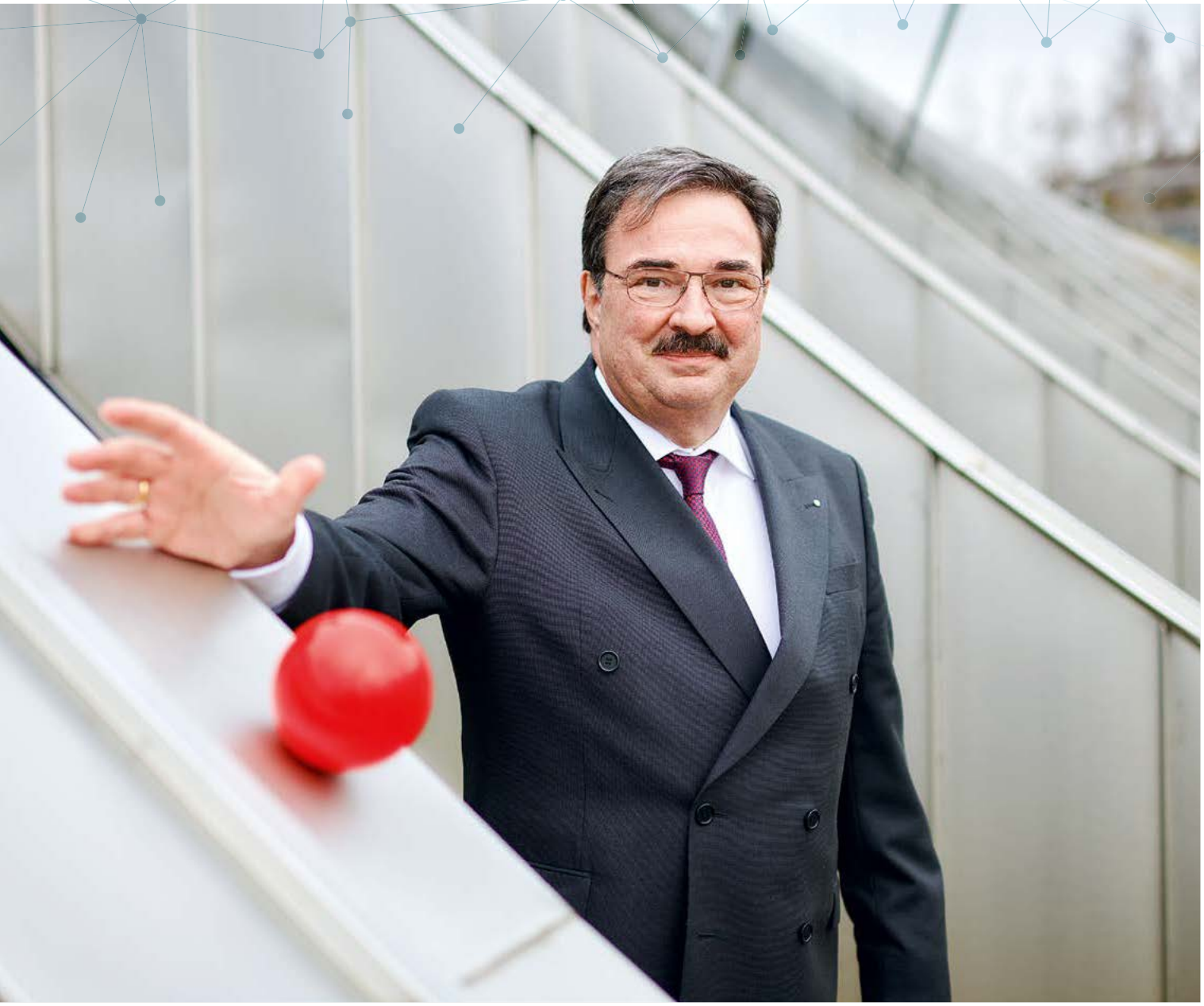

ADOLF J. DOERIG, LEITER ADVISORY BOARD CYBERSECURITY, SATW

Die Schwerpunktthemen der Schweizerischen Akademie der Technischen Wissenschaften (SATW) werden vom Wissenschaftlichen Beirat festgelegt und bezüglich ihrer Bedeutung und Relevanz für die Schweiz stetig überprüft. Seit 2013 zählt das Thema Cybersecurity dazu. Die SATW leistet mit ihren Aktivitäten in den Bereichen Sensibilisierung, Früherkennung und Vernetzung einen Beitrag, dieses wichtige Thema in der Schweiz voranzubringen. So ist sie beispielsweise an der laufenden Ausarbeitung der Nachfolgestrategie zur Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken beteiligt. Gemeinsam mit dem Eidgenössischen Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS) und dessen Expertengruppe Cyber-Defence bearbeitet die SATW zudem das Thema Cyber-Souveränität.

«DAS THEMA CYBERSECURITY MUSS RASCH UND KOMPETENT VORANGEBRACHT WERDEN»

Autor: Adrian Sulzer

«Die Schweiz hat sich früh mit Cybersecurity beschäftigt, zwischendurch aber den strategischen Fokus verloren. Nun gilt es, agil, kreativ, professionell und konsequent auf der Basis einer attraktiven und motivierenden Vision vorwärtszumachen, um den internationalen Anschluss nicht zu verlieren.

ADOLF J. DOERIG ist Maschineningenieur und hat im Nebenfach Kunstgeschichte und Spanisch studiert. Später folgten eine Management-Weiterbildung an der Universität St. Gallen sowie ein Executive MBA an der Universität Zürich. Er ist selbstständiger Unternehmer sowie Berater und leitet aktuell als Präsident die Expertengruppe Cyber-Defence des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS). Bei der Schweizerischen Akademie der Technischen Wissenschaften SATW sitzt er dem Advisory Board Cybersecurity vor. Daneben ist er in verschiedenen nationalen und internationalen Organisationen engagiert.

Wir sind alle digital und somit im globalen Cyberraum vernetzt. Die Digitalisierung fast aller Lebensbereiche schreitet rasant voran und die Schweiz steckt als Dienstleistungs- und Industrienation mittendrin. Vitale Systeme und Prozesse verändern sich mit stetig steigendem Tempo. Entwicklungen in Bereichen wie Blockchain, künstliche Intelligenz und Robotik stellen bestehende Institutionen und Lebensformen vor immer grössere Herausforderungen, insbesondere bezüglich Sicherheit.

Nach meinem Studium zum Maschineningenieur absolvierte ich ein Nachdiplomstudium für Computer Science und System Engineering. Meine technischen Ausbildungen ergänzte und verfeinerte ich fortlaufend, zum Beispiel dank betriebswirtschaftlichen Nachdiplomen. Entscheidend für meine Karriere war aber der Aufbau von Erfahrungswissen in nationalen und internationalen Projekten, hauptsächlich als verantwortlicher Partner bei globalen Beratungsfirmen. Dabei galt immer der Anspruch, technisch anspruchsvolle und kommerziell erfolgreiche Systeme für die Kunden zu bauen. Meine top ausgebildeten, kritischen, kreativen und umsetzungsstarken Mitarbeitenden waren stets der Schlüssel zum Erfolg und mein Ansporn zum fortlaufenden Lernen. Erfahrungen aus leistungsfähigen Teams und schwierigen Projekten sind wahrlich Gold wert. Die meiste Zeit beschäftigten uns komplexe Projekte für Konzerne wie Airbus, UBS, Novartis, Saudi Aramco, Siemens oder SwissRe. Dabei wurde Cybersecurity zunehmend als Teil des Geschäftsmodells verstanden und nicht nur als Kostenfaktor. Inzwischen gilt das dank digitalen Geschäftsmodellen, Advanced Manufacturing oder Industrie 4.0 fast immer. Weiter bauten wir Dienstleistungen für Forensik und Investigation im Cyberraum auf, unter anderem für das Bundeskriminalamt oder Interpol. Das brachte mich noch näher zum Thema Cybersecurity.

So kam es, dass ich in die Planung der strategischen Führungsübung (SFU) 1997 involviert war. Die Schweiz war erst das zweite Land nach den USA, das Szenarien zu Cyberbedrohungen in breit angelegten Führungsübungen behandelte. Die SFU basierte auf Szenarien der amerikanischen RAND Corporation, die erstmals ausserhalb der USA eingesetzt wurden. Zivile, behördliche und militärische Stellen arbeiteten intensiv zusammen, um Chancen und Gefahren der Informationsgesellschaft zu ermitteln. Es ging im Kern um die Robustheit und die Resilienz kritischer Systeme. Vieles, worüber heute diskutiert wird, war damals schon Thema. Aus einer weiteren SFU mit dem Namen «Informo 2001» entstand schrittweise die Melde- und Analysestelle Informationssicherung des Bundes, MELANI. Leider wurden sonst kaum Erkenntnisse oder Empfehlungen der Übungen umgesetzt. So hat die Schweiz ihren Vorsprung beim Thema Cybersecurity verspielt. Wir waren gut im Analysieren, aber etwas träge oder unwillig im Umsetzen. Heute stehen wir vor noch grösseren Herausforderungen. Wir brauchen rasch eine motivierende Vision und eine klare Strategie, um uns im Cyberraum national und international gut zu positionieren. Das Thema Cybersecurity muss rasch, kompetent und lösungsorientiert vorangebracht werden. Die Schweiz geniesst international ein hohes Ansehen und grosses Vertrauen. Darauf könnten wir aufbauen, um uns bezüglich Cybersecurity an die Weltspitze zu setzen. Das ökonomische Potenzial ist enorm.»