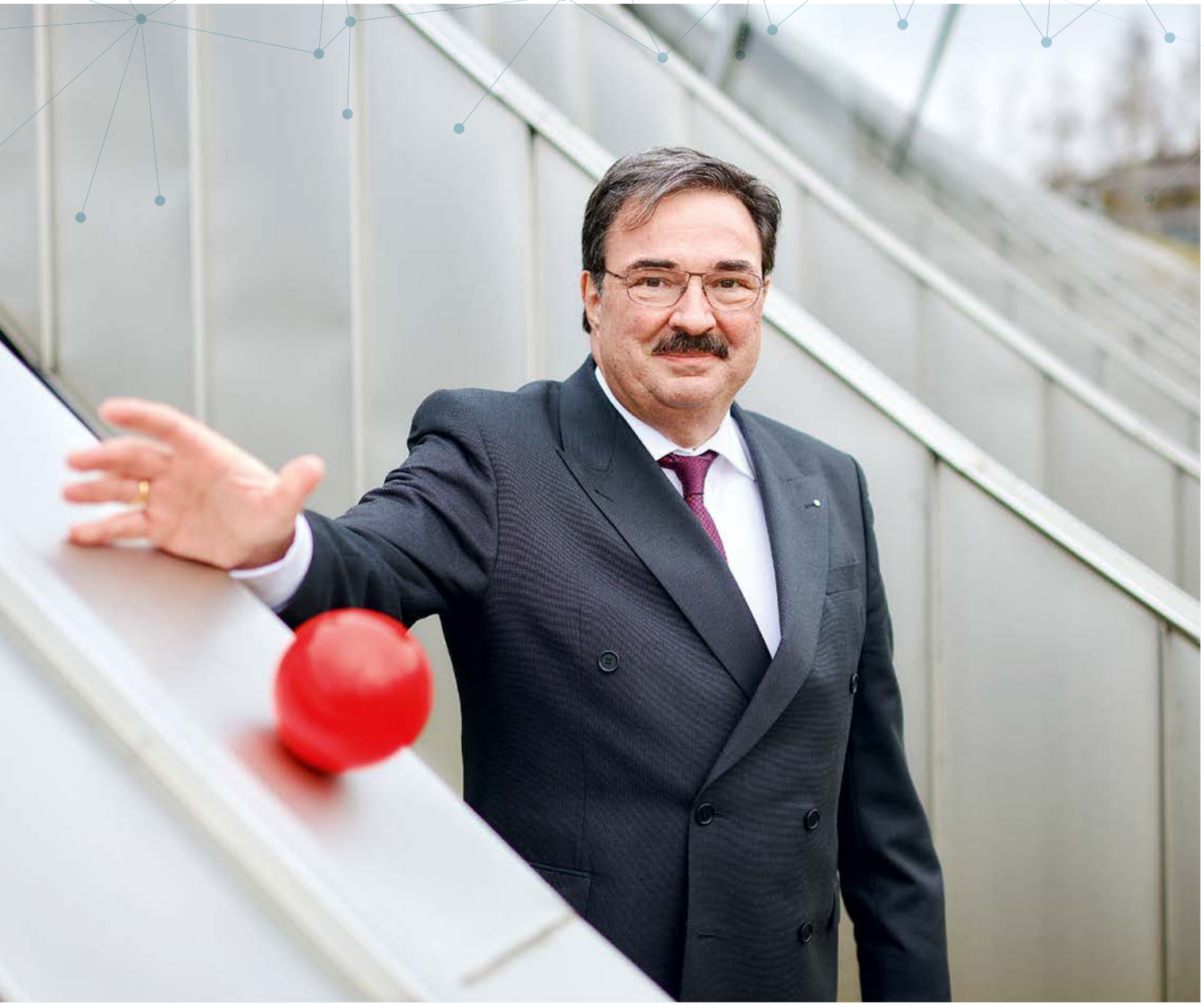

ADOLF J. DOERIG, PRÉSIDENT DU ADVISORY BOARD CYBERSECURITY, SATW

Les thèmes prioritaires de l'Académie suisse des sciences techniques (SATW) sont fixés par le Conseil scientifique. Leur importance et leur pertinence pour la Suisse font l'objet d'un examen régulier. Depuis 2013, le thème de la cybersécurité est l'un d'eux. Grâce à ses activités en matière de sensibilisation, de détection précoce et de mise en réseau, la SATW contribue à développer ce thème important en Suisse. Elle participe ainsi à l'élaboration en cours de la stratégie qui succèdera à la Stratégie nationale de protection de la Suisse contre les cyber-risques. En collaboration avec le Département fédéral de la défense, de la protection de la population et des sports (DDPS) et son groupe d'experts cyberdéfense, la SATW se préoccupe par ailleurs du thème de la cyber-souveraineté.

« LE THÈME DE LA CYBERSÉCURITÉ DOIT ÊTRE DÉVELOPPÉ RAPIDEMENT ET DE FAÇON COMPÉTENTE »

Auteur : Adrian Sulzer

« La Suisse s'est tôt préoccupée de la cybersécurité. Entre-temps, elle a toutefois pâti d'un manque d'orientation stratégique. Il importe maintenant d'avancer sur la base d'une vision flexible, créative, professionnelle et conséquente, afin de ne pas se faire distancer au niveau international.

ADOLF J. DOERIG est ingénieur en mécanique et a étudié l'histoire de l'art et l'espagnol en branches secondaires. Il a ensuite suivi une formation en management à l'Université de Saint-Gall et a effectué un Executive MBA à l'Université de Zurich. Il est entrepreneur indépendant ainsi que conseiller et dirige actuellement le groupe d'experts cyberdéfense du Département fédéral de la défense, de la protection de la population et des sports (DDPS). Il préside l'Advisory Board Cybersecurity de l'Académie suisse des sciences techniques (SATW) et s'engage au sein de diverses organisations nationales et internationales.

Nous sommes tous des êtres numériques et donc connectés au sein de l'espace cybernétique. La digitalisation de presque tous les domaines de la vie progresse rapidement et la Suisse avec ses services et son industrie est particulièrement concernée. Des processus et des systèmes vitaux se modifient à un rythme toujours plus élevé. Des développements dans des secteurs comme les blockchains, l'intelligence artificielle et la robotique placent les institutions et les modes de vie devant des défis toujours plus grands, notamment en matière de sécurité.

Après mes études en génie mécanique, j'ai obtenu un diplôme post-grade en informatique et en ingénierie des systèmes. J'ai ensuite constamment complété et amélioré mes formations techniques, par exemple grâce à des diplômes en gestion d'entreprise. Mais ce qui a été décisif pour ma carrière, c'est l'expérience que j'ai accumulée dans des projets nationaux et internationaux, principalement en tant que partenaire responsable auprès de sociétés de conseil globales. Il s'est agi à chaque fois de mettre sur pied pour des clients des systèmes techniquement exigeants et commercialement fructueux. Mes collaborateurs très bien formés, critiques, créatifs et pleinement opérationnels ont toujours été la clé du succès et une motivation pour continuer à me former. Les expériences engrangées au sein d'équipes efficaces et dans le cadre de projets difficiles valent vraiment de l'or. La plupart du temps, nous nous sommes occupés de projets pour des grands groupes comme Airbus, UBS, Novartis, Saudi Aramco, Siemens ou SwissRe. Dans ce contexte, la cybersécurité a de plus en plus été considérée comme une partie du modèle d'affaires et pas seulement comme un facteur de coût. Grâce aux modèles d'affaires digitaux, à la fabrication de pointe et à l'industrie 4.0, c'est aujourd'hui presque toujours le cas. Nous avons par ailleurs développé des services pour les secteurs de la criminalistique et de l'investigation dans le cyberespace, entre autres pour l'Office fédéral allemand de police criminelle et Interpol. Cela m'a encore davantage familiarisé avec le thème de la cybersécurité.

C'est ainsi que j'ai été impliqué en 1997 dans la planification de l'Exercice de conduite stratégique (ECS). La Suisse était le deuxième pays après les Etats-Unis à intégrer des scénarios de menaces cybernétiques dans des exercices de conduites à large échelle. L'ECS se basait sur des scénarios de la RAND Corporation américaine, qui étaient appliqués pour la première fois à l'extérieur des Etats-Unis. Les instances civiles, étatiques et militaires ont collaboré de manière étroite, afin d'identifier les chances et les risques de la société de l'information. Il s'agissait principalement de tester la solidité et la résistance de systèmes critiques. Beaucoup de choses débattues aujourd'hui étaient déjà à l'ordre du jour. C'est à la suite d'un autre ECS intitulé ‹Informo 2001› qu'a été créée par étapes la Centrale d'enregistrement et d'analyse pour la sûreté de l'information de la Confédération, MELANI. A part cela, peu de connaissances et de recommandations issues des exercices ont malheureusement été mises en pratique. La Suisse a ainsi perdu son avance en matière de cybersécurité. Nous étions bons en ce qui concerne l'analyse, mais un peu indolents et velléitaires pour ce qui est de la mise en œuvre. Aujourd'hui, nous nous retrouvons face à des défis encore plus grands. Nous avons besoin de façon urgente d'une vision stimulante et d'une stratégie claire, afin de bien nous positionner dans le cyberespace national et international. Le thème de la cybersécurité doit être développé de manière rapide, compétente et être axé sur les solutions. La Suisse jouit à l'échelle internationale d'une excellente réputation et d'une grande confiance. Nous pouvons en tirer profit pour nous placer parmi les leaders mondiaux en matière de cybersécurité. Le potentiel économique est énorme. »