Pressemitteilung

Wien, 05.10.2023

IDSF23: ÖSTERREICH ALS HOTSPOT FÜR DIE DIGITALE SICHERHEITSCOMMUNITY

Im Rahmen des 3. International Digital Security Forum (IDSF) trafen unter dem diesjährigen Motto „Digital Resilience – The Basis for a Safe, Secure and Free Society" Akteure der internationalen Digitalisierungscommunity aus rund 35 Ländern zum Dialog in Wien zusammen.

Wien (AIT) – In seiner dritten Auflage stellte das IDSF23 von 19. – 21. September einmal mehr seine Unverwechselbarkeit als internationaler Treffpunkt von Security-Expert:innen an den Schnittstellen von Diplomatie, Politik, IT-Industrie und der Wissenschaft eindrucksvoll unter Beweis. In nur drei Jahren reifte der für das Forum entwickelte „Brand" zu einer global wiedererkennbaren Referenz für den lösungsorientierten und nachhaltigen Multi-Stakeholder-Austausch zu dominierenden Kernthemen digitaler Sicherheit heran.

Die Konferenz wurde als bewährter Mix aus inspirierenden Keynotes und hochkarätig besetzten Diskussions-Panels konzipiert. Insgesamt konnte das ISDF23 mit 8 Keynotes und 13 Sessions aufwarten, an denen insgesamt mehr als 100 Sprecher:innen beteiligt waren. Über 500 Teilnehmer:innen besuchten an den 3 Tagen das IDSF als internationalen Hotspot für die digitale Sicherheit.

„Wir sind sehr stolz darauf, dass es uns in so kurzer Zeit gelungen ist, für die Bewältigung der Herausforderungen unserer digitalen Transformation eine einzigartige Community aus Diplomatie, Politik, IT-Industrie und Wissenschaft zusammenzubringen", so Helmut Leopold, der Initiator des IDSF.

Der Erfolg des IDSF verdankt sich breiter internationaler Unterstützung und Kooperation

Das vom AIT Austrian Institute of Technology in Zusammenarbeit mit der ARGE Sicherheit und Wirtschaft (ASW) der Wirtschaftskammer Österreich und dem Kompetenzzentrum Sicheres Österreich (KSÖ) organsierte IDSF konnte die Attraktivität der Programminhalte an den drei Konferenztagen nicht zuletzt im Hinblick auf die breite öffentliche Unterstützung im In- und Ausland gegenüber letztem Jahr weiter steigern.

Ergänzend zur österreichischen Bundesadministration mit Bundeskanzleramt, Bundesministerium für europäische und internationale Angelegenheiten, Bundesministerium für Inneres, Bundesministerium für Finanzen mit dem Staatssekretariat für Digitalisierung und Telekommunikation und Bundesministerium für Landesverteidigung haben internationale Organisationen wie die Vereinten Nationen, die OSCE und die IAEA dem Forum ebenso unterstützend zur Seite gestanden, wie namhafte Industriesponsoren (SAAB COMBITECH, msg Plaut und Trend Micro Austria), sowie Raiffeisen als Location-Host der Konferenz.

Im Interesse einer möglichst umfassenden Abdeckung aktueller Herausforderungen rund um die Etablierung von digitaler Resilienz der Wirtschaft, der Behörden als auch der Gesellschaft, erörterte die Konferenz folgende Themen in Schlüsselbereichen der Digitalisierung und damit zusammenhängender Sicherheitsfagen:

- TechDiplomacy und damit verbundene verantwortliche Technologieentwicklung und Umgang mit sensiblen Daten im globalen Kontext
- Einsatz von vertrauenswürdiger Künstlicher Intelligenz (KI)
- Digitalisierung für ein modernes Krisen-, Konflikt- und Katastrophen-Management
- Vorantreiben digitaler Sicherheit durch digitale Innovation
- Cybersicherheit für kritische Infrastrukturen

Ergänzend zum Dialogforum führte analog zum Vorjahr der IDSF-Partner VICESSE (Vienna Centre for Societal Security) am mittleren Konferenztag eine parallele, eigene Tagung für die internationale Wissenschafts-Community zum Thema „(De-)Zentralisierung digitaler Infrastrukturen“ durch.

Internationale Bedeutung des IDSF

Am Dienstag, dem 19. September 2023, um 14:00 Uhr, eröffnete Helmut Leopold, Initiator des ISDF und Leiter des Center for Digital Safety & Security am AIT, auch in Vertretung und im Auftrag des Bundeskanzlers der Republik Österreich, Karl Nehammer, die dritte Auflage des Forums, welches heuer erstmals als reine Präsenzveranstaltung im Raiffeisen Forum Wien über die Bühne ging.

Im Anschluss daran richtete der im Vorjahr persönlich anwesende, jedoch wegen der zeitgleichen Abhaltung der UN-Vollversammlung in New York nur mittels Videogruß-Botschaft präsente Raffi Gregorian, Deputy to the Under-Secretary-General and Director United Nations Office of Counter-Terrorism (UNOCT), einen eindringlichen Appell an die Teilnehmer:innen des IDSF, globale kritische Infrastrukturen in gemeinsamer Anstrengung zu schützen und dabei Menschenrechte bestmöglich zu respektieren und unterstrich die bereits etablierte, gute Kooperation zwischen der UN und dem AIT.

Danach gab Spanien, das derzeit nach dem halbjährigen Rotationsprinzip den Ratsvorsitz in der Europäischen Union innehat, dem Forum durch den Auftritt seiner Botschafterin in Österreich, Cristina Fraile, die Ehre. Sie skizzierte in ihrer Eröffnungsrede die Schwerpunktsetzungen ihres Landes für die weitere europäische Digitalisierungspolitik wie z.B. digitalisierte Re-Industrialisierung und Umsetzung wichtiger Rechtsakte wie „AI Act“, die Konsolidierung der Europäischen Digitalen Identität oder den „Cyber Resilience Act. Sie begrüßte auch ausdrücklich die Erteilung eines neuen Mandats an die European Union Agency for Cybersecurity (ENISA) mit Einführung des Cyber Security Acts als EU-weitem Zertifizierungsrahmen für eine Steigerung der Cybersicherheit im Frühjahr dieses Jahres.

Die Konferenzeröffnung wurde durch eine Keynote von Bjørn Berge, Deputy Secretary General of the Council of Europe (CoE), Strasbourg, abgerundet. In seiner Rede erläuterte er die Rolle des

Council of Europe in der globalen Governance für AI und andere aufkommende Technologien und ging auf ihre geopolitischen Auswirkungen ein. Für ihn stellen die größten Herausforderungen die Gegenwehr zu Cyber Crime, der Datenschutz und mit diesem das Recht auf ein Privatleben und menschliche Würde sowie die Entwicklung einer menschen-zentrierten Künstlichen Intelligenz dar.

Verantwortungsvolle Technologie-Entwicklung, Künstliche Intelligenz

Im ersten Panel im Track 1 „Responsible Technology Development" mit Claudia Reinprecht, Head of Department for Telecommunications, Digital and Tech Diplomacy im BMEIA, als Chair, beleuchteten Sicherheits-Expert:innen das Thema „Tech-Diplomatie im 21. Jahrhundert" aus geopolitischer Sicht. Ausgehend von der Erkenntnis, dass Technologien kritische Faktoren für die Innovations- und Wettbewerbsfähigkeit sowie die nationale Sicherheit und militärische Stärke von Staaten sind, kamen das nicht immer friktionsfreie Verhältnis von Unternehmen, Regierungen und Gesellschaften im digitalen Raum ebenso zur Sprache, wie die Entwicklung von Strategien zur globalen Regulierung und Governance der für politisches Power-Play genutzten Schlüsseltechnologien, wie z.B. Künstliche Intelligenz und Quantentechnologien.

Die Überleitung zum Session Track 2 „Artificial Intelligence" lieferte der Rektor des Instituts für die Wissenschaft vom Menschen (IWM), Misha Glenny, mit seiner philosophisch unterfütterten Keynote über „AI, Cybercrime and Human Scale". Er zeigte auf, wie dramatische und politische Umbrüche in der Vergangenheit immer auch zu tiefen technologischen Veränderungen führten und es der Menschheit dabei zunehmend schwerfiel, eine Balance zwischen Fortschritts- und menschlichen Erfordernissen zu finden. Im Lichte der immer größeren Macht und Allgegenwärtigkeit von Künstlicher Intelligenz und ihrer Nutzung für Cybercrime, brauchen wir dringend die Rückkehr zu menschlicher Kontrolle über unsere Technologien.

Der erste Konferenztag ging mit dem Panel über „Trustworthy and Socially Responsible AI" zu Ende. Dabei wurde der Themenbogen von Informationsintegrität und Bias-Vermeidung über eine Sicherstellung der Transparenz von KI-Algorithmen, eine notwendige breite öffentliche Grundbildung bis hin zu Desinformationsbekämpfung mittel AI in der Nachrichtenwelt gespannt. Nachverfolgbarkeit und Erklärbarkeit KI-gestützter Systemvorgänge sind unbedingt erforderlich, um das Vertrauen in Maschinen zu verbessern und die Lücke zu einem KI-Verständnis weiter zu schließen.

Modernes Krisen-, Konflikt- und Katastrophen-Management und verbesserte globale Sicherheit durch digitale Technologien

Der zweite Konferenztag wurde mit einer Eröffnungsrede von Josef Schröfl, Deputy Director, CoI on Strategy and Defense and Head of Cyber Workstrand beim European Centre of Excellence for Countering Hybrid Threats, Helsinki, Finnland, eingeleitet. Er merkte mit Blick auf den Ukraine-Krieg an, dass es bei der neuen Art der Kriegsführung mit massenhaften Desinformationskampagnen und gezielten Versuchen, kritische digitale Infrastrukturen mit Cyberangriffen zu attackieren, nicht mehr ausreiche, sich ausschließlich militärisch zu verteidigen, sondern dass die parallele und effektive Verteidigung des Cyber Space unerlässlich geworden ist.

Im Anschluss gab Lars van Dassen, Executive Director, World Institute for Nuclear Security (WINS), in der ersten Keynote des Tages Einblick in den Betrieb kritischer Infrastrukturen in

schwierigen Umgebungen am Beispiel der Ukraine. Er zeigte eindrucksvoll auf, in welch schwierigen und äußerst belastenden Situationen Menschen in ihrem Kampf für Demokratie und Freiheit höchsten Einsatz erbringen, um einen sicheren Betrieb von kritischen Infrastrukturen aufrecht zu erhalten.

Danach adressierte Session Track3 zuerst die durch digitale Innovationen eingeläutete Transformation des Krisen- und Katastrophenmanagements und die damit entstandenen Möglichkeiten, auf transnationale Bedrohungen besser und abgestimmter reagieren zu können. Danach wurde erörtert, wie eine moderne Digitalisierung durch Verwendung von z.B. sozialen Medien, geografischen Informationssystemen, Datenanalyse und virtuellen Trainingstechnologien dazu genutzt werden kann, eine Steigerung der Sicherheit bei Friedensmissionen auf hybriden Krisenschauplätzen zu erreichen und die vielfältigen internationalen Bemühungen im zivilen Krisen- und Konfliktmanagement besser zu unterstützen.

Der Nachmittag wurde mit einer Keynote in Form einer vorbereiteten Videopräsentation durch Guilherme Canela Godoi, Chief of the Section of Freedom of Expression and Safety of Journalists am UNESCO Headquarter, Paris, eingeleitet. Er ging dabei auf die globale „Internet4Trust“-Initiative der UNESCO ein, die in gemeinsamer, globaler Anstrengung Guidelines für definierte Prinzipien und Prozesse der Content-Moderation und -kuration unter Berücksichtigung der Menschenrechte und der freien Meinungsäußerung im digitalen Raum entwickeln will.

Im darauffolgendem Session Track 4 „Advancing Global Security Through Digital Innovations” wurden nacheinander Tools, Technologien und Strategien zur Bekämpfung des Organisierten Verbrechens sowie Innovationen und Services für Counter-Terrorism-Strategien diskutiert. In der ersten Diskussion ging es vorrangig um diverse Grenzsicherungsmaßnahmen durch Strafverfolgsbehörden, im zweiten wurde das CT (Countering Terrorist) Travel Programm von UNOCT (United Nations Office of Counter Terrorism) im Detail vorgestellt. Die dritte Panel-Runde befasste sich mit verantwortlichem digitalen Identitätsmanagement, wo Sicherheitsstandards zum Schutz vor Missbrauch, sowie technologische Lösungen für einen verbesserten Schutz der Privatsphäre und echten Datenschutz diskutiert wurden.

Die dritte und letzte Keynote des mittleren Konferenztages kam von Ludmyla Rabchynska, CGI Executive Consultant und OECD Consultant, sowie frühere stellvertretende Ministerin für die digitale Transformation in der Ukraine. Sie gab einen Einblick in die seit Jahren von Russland systematisch versuchte Zerstörung der kritischen Infrastruktur der Ukraine. Hauptziele dabei waren Regierungseinrichtungen, Informations- und Energiesysteme, Telekommunikation und Finanzzentren. Zwischen 2013 und 2021 wurden in der Ukraine rund 40 Millionen Cyber-Vorfälle registriert, die auf russische Spionage, Unterbrechung von Informationsdiensten und versuchte informationspsychologische Einflussnahme zurückgehen.

Im letzten Panel des Tages wurden Technologie-Förderungssysteme und Partnerschaften vorgestellt. Zuerst ging Ralph Hammer, Director of the Staff Department for Security Research and Technology Transfer im Bundesministerium für Finanzen, auf die neben dem KIRAS- und FORTE-Forschungsprogramm jetzt neu ins Leben gerufene Sonderrichtlinie „K-PASS“ (Kybernet-Pass) ein, mit der erstmals ein vollständig auf Cyber-Sicherheit ausgelegtes Forschungsförder-

Instrument, welches EU-weit beispielhaft ist, in Österreich etabliert wird. Danach erläuterte Lydia Lindner von der Österreichischen Forschungsförderungsgesellschaft FFG die europäischen Förderprogramme, welche eine wichtige Rolle zur Etablierung eines notwendigen Innovations-Öko-Systems für die digitale Sicherheit in der EU darstellen.

Cybersicherheit für kritische Infrastrukturen

Der Schlusstag der Konferenz wurde mit einer Video-Grußbotschaft des Innenministers der Republik Moldavien, Adrian Efros, eröffnet, der vor allem die notwendige Kooperation zwischen den europäischen Nationen hervorstrich, um eine gemeinsame Sicherheitsdoktrin auch für den digitalen Raum zu etablieren.

Danach präsentierte Dominika Hajdu, Director of the Centre Democracy and Resilience beim slowakischen Think Tank GLOBSEC in Bratislava, in ihrer Keynote “A never ending battle: How to build and maintain societal resilience to foreign malign influence” Ergebnisse durchgeführter Studien zu sich entwickelnden und verfestigenden gesellschaftlichen Meinungsbildern über den Ukraine-Krieg im Hinblick auf gestreute Desinformation. Sie zeigte Wege auf, wie sich unsere demokratischen Gesellschaften dagegen aufstellen können.

Der restliche Vormittag beleuchtete mit 3 Panels unterschiedliche Fragestellungen des Session Tracks 5 „Cyber Security“.

Im ersten ging es um die disruptive Herausforderung der Etablierung verlässlicher und sicherer Datenaustausch-Ökosysteme, mit denen das aus Sicht unterschiedlicher Industrien notwendige Vertrauen in verwendete Infrastrukturen, involvierte Akteure und angewandte und Datenaustauschmechanismen auf- und ausgebaut werden kann.

Das zweite mit u.a. Walter Fraißler, Head of Information Security, Verbund AG, Austria und Wolfgang Rosenkranz, Team Leader Austrian Energy CERT, Austria, als teilnehmende Diskutanten zum Thema „Securing the Energy Sector: Strategies for Building Resilience against Cyber Attacks“ kam einem kleinen Energie-Gipfel gleich, und brachte die ganze Palette aktueller Herausforderungen wie Network Monitoring, Incident Response, Continuity Management und Recovery sowie Überwindung der Supply Chain-Unsicherheiten durch Einsatz neuer IT- und OT-Technologien aus der Cloud zur Sprache. Aus wissenschaftlicher Perspektive brauche es zudem verstärkte Forschung zur Entwicklung modernster Schutzmethoden, um den steigenden Bedrohungen effektiv entgegen zu wirken.

Das den Vormittag beschließende Panel befasste sich unter dem Titel „Bridging the Gap: Strategies for Global Collaboration between Security, Standardization and Policy Making Communities“ mit Strategien der Verschränkung dieser Building Blocks. Der Bogen der Diskussion spannte sich, ausgehend von der Automobilindustrie, in der Produktzulassungen bereits mit den regulativen Vorgaben verknüpft sind, über die Cyber Security-Zertifizierung von Produkten und IoT-Systemen bis hin zur Bedeutung von „Security by Design“ für die Entwicklung resilienter Systeme. Die Session nahm auch auf die NIS2 Direktive Bezug und hob ihre Relevanz für die Etablierung von Cyber Security Standards hervor.

Die abschließende Etappe des IDSF gestaltete sich zu einem wahren „Endspurt of Excellence“ und dies sowohl aus politischer, wirtschaftlicher und auch wissenschaftlicher Perspektive.

Zu Beginn des Nachmittags beleuchtete Florian Tursky, Staatssekretär für Digitalisierung und Telekommunikation im Bundesministerium für Finanzen (BMF) in seiner Keynote „The Importance of Digital Transformation“ wie wir alle den Shift in die digitale Welt, die Verlagerung unseres Lebens ins Internet meistern können. Für ihn stellen die tragenden Säulen „Collaboration“, „Skills“ und natürlich die intensive Auseinandersetzung mit Künstlicher Intelligenz sowie ihre menschengerechte Regulierung eine richtig verstandene und exekutierte digitale Transformation dar, wie dies in Europa mit dem kommenden AI Act adressiert wird, auch um bestehende Ängste in der Bevölkerung abzubauen.

Die finale Keynote der Konferenz „Unlocking and Protecting Value: Transforming Industrial Ecosystems and Smart Cities with Cybersecurity Vigilance” von Senadin Alisic, Strategy Advisor, Combitech AB, Schweden, betonte die Wichtigkeit der neu entstehenden Datenökonomie, welche existierende Geschäftsmodelle grundlegend verändern wird und stellte drei eindrucksvolle Data-Space Beispiele in den Bereichen Smart City, nachhaltiger Bergbau und effektivster Logistikbetrieb eines Hafens vor.

Das vorletzte Panel der Konferenz „Building Cyber Resilience: National Strategies for Capacity Development in Cyber Security” diskutierte mit Expert:innen aus der Europäischen Cyber Security Arena die große Herausforderung der Entwicklung der notwendigen Fähigkeiten für kritische Infrastrukturbetreiber, von Behörden und schließlich der gesamten Wirtschaft. Dazu wurden die entsprechende Trainingsinitiativen und Trainingsmethoden der IAEA, UN Office for Counter Terrorism, als auch die neue Initiative zur Umsetzung einer EU Cyber Security Skill Academy vorgestellt.

Das Panel „Navigating the EU Data Strategy: Challenges and Opportunities for Industry and Public Authorities” diskutierte die aktuellen Strategien und Entwicklungen zur Schaffung moderner föderierter IT-Architekturen, welche einen souveränen und vertrauenswürdigen Datenaustausch unterstützen, um auch neue datengesteuerte Geschäftsfälle voranzutreiben.

Dabei wurde auch die EU Gaia-X Initiative erörtert, welche sich mit der Entwicklung technischer Open-Source-Lösungen sowie der Etablierung offener Spezifikationen beschäftigt, um eine offene und standardisierte Systemarchitekturentwicklung für föderierte Datenaustauschplattformen zur Bildung effektiver „Datenräume“ in verschiedenen Marktsegmenten zu ermöglichen.

Die Schlussansprache des IDSF23 blieb Karoline Edtstadler, Bundesministerin EU und Verfassung im Bundeskanzleramt, vorbehalten. Sie formulierte das österreichische Verständnis eines offenen, freien, sicheren und globalen Internets, für das als Gradmesser zu aller erst immer die Menschenrechte gelten. Dabei verwies sie auf die wichtige Verzahnung von Politik, Wissenschaft und Gesellschaft. In ihrer Rede gab sie auch tiefen Einblick in ihre Arbeit beim „Leadership Panel“ des bei den UN angesiedelten „Internet Governance Forums (IGF)", in das sie im Vorjahr von UN General Secretary Antonio Guterres als eines von 10 Mitgliedern für einen zweijährigen Term ernannt worden ist.

Paralleler Social Science Track am mittleren Konferenztag

Auch beim IDSF23 wurde die im Vorjahr begonnene erfolgreiche Zusammenarbeit mit dem Vienna Centre for Societal Security (VICESSE) mit einem am Mittwoch, 20. September 2023, parallel zum IDSF-Hauptprogramm abgehaltenen „Social Science Track“ erfolgreich fortgesetzt. Das Meta-Thema „(De-)Centralization of Digital Infrastructures“ wurde in Form von 2 Keynotes und vier thematischen Sessions reflektiert, die sich mit den Subthemen „Dezentralisierung, Open Source und Open Data“ zu einem inhaltlichen Nexus zusammenfügten.

Anja Klauzer und Veronika Nowak von SBA Research rissen in ihrer Keynote die Bedeutung von „Open Source Intelligence für Energieinfrastrukturen“ an und Jeanette Klonk von der FFG beleuchte den Themenkomplex „Forschung und Innovation für eine offene, inklusive und sichere Gesellschaft“.

Die drei über den Tag verteilten Sessions „Digital Infrastructures and Supply Infrastructures”, „The power of Social Media Platforms“ und “Digital Infrastructures of governance” beleuchteten wichtige Aspekte der laufenden Infrastruktur-Diskussion und ein abschließender Round-Table zum Thema “Hypercriticality: Establishing Safety & Security of entangled infrastructures” fasste die Herausforderungen der dichten Verschränkung von kritischen, digitalen Infrastrukturen noch einmal im großen Bild zusammen.

Begleitende Ausstellung innovativer österreichischer KMUs und globaler Unternehmen

Das ISDF setzte 2023 auch die Tradition einer begleitenden Ausstellung fort, bei der innovative heimische Unternehmen (KMUs) und Organisationen der IT-Branche, als auch Forschungseinrichtungen ihre Entwicklungen einem interessierten und versierten Fachpublikum präsentieren konnten. Aussteller in diesem Jahr waren die Austrian Defense and Security Industry Group (ASW) der Wirtschaftskammer Österreich, das Kompetenzzentrum Sicheres Österreich (KSÖ), SAAB COMBITECH, msg Plaut, Trend Micro Austria, X-Net Services, Misbar, Nimbusec, Bacher Systems, fragmentiX, Cyttraction, Rohde & Schwarz, Sustainista, SBA Research, Digital Factory Vorarlberg, Silkroad 4.0, Vienna Cyber Security and Privacy Research Cluster (VISP) und die Vienna Business Agency.

Namhafte Sponsoren als Unterstützer des IDSF

SAAB COMBITECH war der europäische Industrie-Hauptsponsor des International Digital Security Forums Vienna 2023. Raiffeisen unterstützte das IDSF großzügig mit der Bereitstellung der Event-Location „Raiffeisen Forum“ Wien. Weitere Sponsoren und Unterstützer waren das Kompetenzzentrum Sicheres Österreich (KSÖ), die ARGE Sicherheit und Wirtschaft (ASW) der Wirtschaftskammer Österreich, die DigitalCity.Wien Initiative, die Österreichischen Sicherheitsforschungsprogramme KIRAS und FORTE, AED, msg Plaut, Trend Micro Austria, Verbund, World Institute of Nuclear Security (WINS), The European Security and Defense College, die Vienna Business Agency und wichtige österreichische Bundesministerien. Die Organisatoren der Konferenz bedanken sich bei allen unterstützenden Partner:innen, deren Beitrag ganz wesentlich für die hohe Qualitätsstufe dieser Konferenz war.

IDSF war auch heuer Green Event

Das “International Digital Security Forum Vienna 2023” war erneut gemäß den Richtlinien für Green Meetings & Green Events zertifiziert.

IDSF zum Nachschauen!

Demnächst werden die Video-Mitschnitte aller Keynotes und Sessions sowie ausgewählte Präsentationen des IDSF23 auf der Forum-Webseite http://idsf.io allen registrierten Teilnehmer:innen zur Nachschau zur Verfügung stehen. Interessierte, welche die Konferenz in Wien nicht besuchen konnten und noch nicht registriert sind, können dies in Kürze auf der Website vornehmen und haben damit auch Zugang zu den gesamten Inhalten. Fotos der Veranstaltung sind bereits auf der Forum-Website unter https://idsf.io/impressions-2023/ verfügbar und unter Angabe des Copyright-Hinweises *IDSF/Katharina Schiffl* verwendbar.

Pressekontakt:

Mag. (FH) Michael W. Mürling
Head of IDSF Event Organization
Marketing and Communications
AIT Austrian Institute of Technology
Center for Digital Safety & Security
T +43 (0)50550-4126
michael.muerling@ait.ac.at I www.ait.ac.at

Mag. Michael H. Hlava
Head of Corporate and Marketing Communications
AIT Austrian Institute of Technology
T +43 (0)50550-4014
michael.hlava@ait.ac.at I www.ait.ac.at