digiVolution
Prepare for the next

dV-News

Les billets de *digi*Volution / *digi*Volution's Newsletters
[17.01.2024 – Édition / Ausgabe Nr. 93]

dVCyberGroup is born

Chers Lectrices et Lecteurs

Voici les **dV-News 02-2024** et leur sélection d'articles et liens et le plaisir d'annoncer une naissance.

*digi*Volution s'est donnée pour mission d'observer, de comprendre la mutation numérique et ses défis, principalement sous l'angle de la sécurité, et de transmettre ce savoir aux décideurs. Peu après ses débuts, s'est imposée la nécessité de réaliser aussi des projets concrets et, finalement, que *digi*Volution avait besoin pour cela d'un bras opérationnel séparé. Ainsi a été créé en août 2023 la société **dVCyberGroup SA** avec un nom et un slogan qui ne laissent aucun doute sur ses buts et l'idéal qui est poursuivi.

Liebe Leserinnen und Leser

Hier sind die **dV-News 02-2024** und eine Auswahl an Artikeln und Links, und die Freude, eine Geburt zu verkünden.

*digi*Volution hat es sich zur Aufgabe gemacht, die digitale Mutation und ihre Herausforderungen zu beobachten, zu verstehen, vor allem aus dem Blickwinkel der Sicherheit, und dieses Wissen an Entscheidungsträger weiterzugeben. Kurz nach dem Start wurde klar, dass *digi*Volution auch konkrete Projekte durchführen musste und schliesslich einen eigenen operativen Arm benötigte. So wurde im August 2023 die **dVCyberGroup AG** mit einem Namen und einem Motto gegründet, die keinen Zweifel an den Zielen und dem Ideal lassen, das verfolgt wird.

dVCyberGroup
in the spirit of *digi*Volution

Vous en apprendrez plus sur son site Internet https://dvcybergroup.ch dès la semaine prochaine. Il fallait ensuite un patron à *d*VCyberGroup et nous avons le grand plaisir d'annoncer que **M. Haris Stucki** en assure la direction depuis le 1er janvier 2024.

Weitere Informationen finden Sie ab nächste Woche auf der Internetseite unter https://dvcybergroup.ch. Die *d*VCyberGroup brauchte dann einen Chef und wir freuen uns, Ihnen mitteilen zu können, dass **Herr Haris Stucki** seit dem 1. Januar 2024 die Leitung übernommen hat.

Pendant que le *digi*Volution produira de nouveaux savoirs et de nouvelles idées pour maîtriser les défis de la mutation numérique, *d*VCyberGroup produira des prestations au niveau stratégique dans les domaines du conseil, du soutien opérationnel et de la formation. Ce tandem de ***think tank*** et de ***do tank*** aura fort à faire pour fournir aux décideurs de solides bases décisionnelles.

Et quoi de plus difficile lorsque l'on songe aux incertitudes de l'IA? La plus grande enquête du genre vient en effet de demander à 2'778 chercheurs ayant publié dans des revues d'IA de premier plan leurs prévisions sur le rythme des progrès de l'IA et leur impact.

Während die Stiftung *digi*Volution neues Wissen und neue Ideen zur Bewältigung der Herausforderungen der digitalen Mutation entwickelt, wird die *d*VCyberGroup Leistungen auf strategischer Ebene in den Bereichen Beratung, operative Unterstützung und Ausbildung erbringen. Dieses Tandem aus ***Think Tank*** und ***Do Tank*** wird alle Hände voll zu tun haben, um den Entscheidungsträgern solide Grundlagen zu bieten.

Und was könnte schwieriger sein, wenn man an die Unwägbarkeiten der KI denkt? In der grössten Umfrage dieser Art wurden 2'778 Forscher, die in KI-Zeitschriften veröffentlichten, nach ihren Prognosen über das Tempo des KI-Fortschritts und dessen Auswirkungen befragt.

50 % attendent des progrès très significatifs d'ici 2028 déjà. Si le rythme se maintien, 10% estiment probable que des machines autonomes surpassent les humains dans toutes les tâches possibles d'ici à 2027. 50 % d'ici à 2047, soit 13 ans plus tôt que la précédente enquête de 2022. La probabilité que toutes les professions humaines deviennent entièrement automatisables devrait atteindre 10 % en 2037 et 50 % en 2116. 68,3 % des personnes interrogées pensent qu'une IA « surhumaine » a plus de chances de produire de bons résultats que de mauvais.

50% erwarten bereits bis 2028 sehr bedeutende Fortschritte. Bei gleichbleibendem Tempo halten es 10 % für wahrscheinlich, dass autonome Maschinen den Menschen bis 2027 in allen möglichen Aufgaben übertreffen werden. 50 % bis 2047, 13 Jahre früher als bei der letzten Umfrage im Jahr 2022. Die Wahrscheinlichkeit, dass alle menschlichen Berufe vollständig automatisierbar werden, wird auf 10 % im Jahr 2037 und 50 % im Jahr 2116 geschätzt. 68,3 % der Befragten glauben, dass eine «übermenschliche» KI eher gute als schlechte Ergebnisse liefern wird.

Sous un angle plus dystopique, 38 % à 51 % des personnes interrogées estiment à au moins 10 % la probabilité que l'IA conduise à l'extinction de l'humanité. Plus de la moitié ont formulé des inquiétudes « importantes » ou « extrêmes » dans six scénarii, dont la désinformation, le contrôle autoritaire et les inégalités.

En bref, le **principe de précaution devra s'imposer dans tous nos progrès liés à l'IA** ces prochaines années. En espérant que tout le monde joue avec les mêmes règles.

In einer eher dystopischen Perspektive schätzten aber 38% bis 51% der Befragten die Wahrscheinlichkeit, dass die KI zum Aussterben der Menschheit führen wird, auf mindestens 10%. Mehr als die Hälfte der Befragten äusserte «grosse» oder «extreme» Bedenken in sechs Szenarien, darunter Desinformation, autoritäre Kontrolle und Ungleichheit.

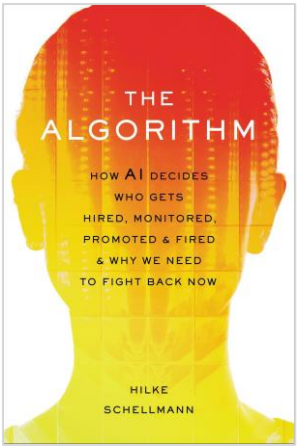
Kurz gesagt, **das Vorsorgeprinzip wird in den nächsten Jahren bei allen unseren KI-bezogenen Fortschritten zum Tragen kommen müssen**. In der Hoffnung, dass alle nach den gleichen Regeln spielen.

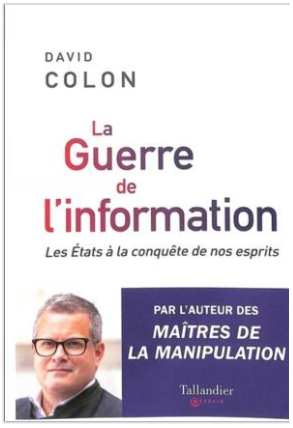
BOOKS & REPORTS

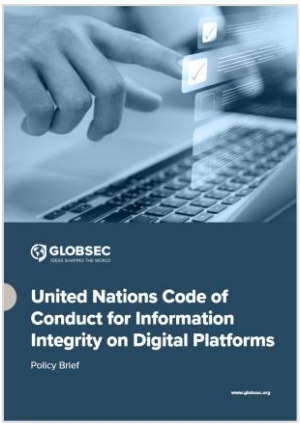
Voici la liste des livres et publications d'intérêt découverts lors de nos recherches durant les deux dernières semaines. La rubrique dVLibrary sera prochainement à disposition des abonnés de dVPedia Pro.

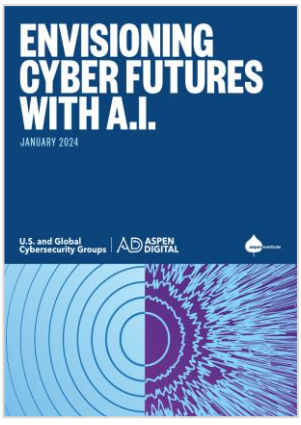
BOOKS & REPORTS

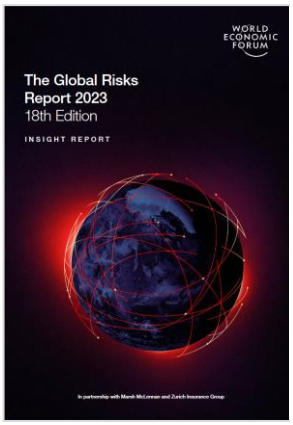
Hier die Liste der Bücher und Publikationen von Interesse, die wir bei unseren Recherchen in den letzten zwei Wochen entdeckt haben. Die neue Rubrik dVLibrary wird in Kürze den Abonnenten von dVPedia Pro zur Verfügung stehen.











News significatives de la quinzaine

► **Les Forces aériennes (FA) suisses indirectement touchées par une cyberattaque** – Les attaques contre Xplain puis contre Concevis en 2023 avaient montré les conséquences d'une attaque contre la chaîne d'approvisionnement. Avec l'attaque du groupe criminel Alphv contre la société américaine Ultra Intelligence & Communications, ce sont cette fois nos FA qui sont touchées et il faudra attendre les résultats d'analyse pour mesurer la réelle gravité de la situation. La question sur toutes les lèvres c'est « comment sécuriser durablement des informations le long de toute une chaîne d'approvisionnement par nature hétérogène? ». Et la question que personne ne veut poser c'est « et comment corriger le passé? », car ces exemples ne sont que la pointe d'un immense iceberg. Alors sommes-nous condamnés à subir un cas après l'autre? Les autorités américaines avaient annoncé avoir neutralisé ce groupe criminel… et il est revenu quelques jour plus tard en jurant vouloir désormais tirer sur tout ce qui bouge, hôpitaux compris. Bonne année !

► **Global Risks Report et Global Cybersecurity Outlook 2023 du WEF** – Les amateurs de vin attendent le Beaujolais nouveau. Chaque année en janvier, les experts en sécurité attendent le dernier Global Risks Perception Survey (GRPS). Nous en avons extrait une phrase qui dit tout: « *Le développement et le déploiement rapides de nouvelles technologies, souvent accompagnés uniquement de protocoles limités pour régir leur utilisation, posent leur propre risques. L'imbrication croissante des technologies dans le fonctionnement essentiel des sociétés expose les populations à des menaces intérieures directes, y compris celles qui cherchent à briser le fonctionnement de la société. Parallèlement à l'augmentation de la cybercriminalité, les tentatives visant à perturber les ressources et les services critiques basés sur les technologies deviendront plus courantes, avec des attaques anticipées contre l'agriculture et l'eau, les systèmes financiers, la sécurité publique, les transports, l'énergie et les infrastructures de communication nationales, spatiales et sous-marines* ».

Wichtige Nachrichten der letzten Wochen

► **Schweizer Luftwaffe (LW) indirekt von Cyberattacke betroffen** – Die Angriffe auf Xplain und Concevis im Jahr 2023 zeigten, welche Folgen ein Angriff auf die Lieferkette haben kann. Mit dem Angriff der kriminellen Gruppe Alphv auf die amerikanische Firma Ultra Intelligence & Communications ist diesmal unsere LW betroffen und es wird die Ergebnisse der Analysen abwarten müssen, um den wahren Ernst der Lage zu ermessen. Die Frage, die in aller Munde ist, lautet: «Wie kann man Informationen entlang einer heterogenen Lieferkette dauerhaft sichern?». Und die Frage, die niemand stellen will, lautet: «Und wie kann man die Vergangenheit korrigieren?», denn diese Beispiele sind nur die Spitze eines riesigen Eisbergs. Sind wir also dazu verurteilt, einen Fall nach dem anderen zu ertragen? Die US-Behörden gaben bekannt, dass sie diese kriminelle Gruppe neutralisiert hatten… und diese kam einige Tage später zurück und schwor, dass sie von nun an auf alles schiessen würden, was sich bewegt, einschliesslich Spitäler. Frohes Neues Jahr!

► **WEF Global Risks Report 2023** – Weinliebhaber warten auf den Beaujolais Nouveau. Jedes Jahr im Januar warten die Sicherheitsexperten auf die neueste Global Risks Perception Survey (GRPS). Wir haben einen Satz herausgegriffen, der alles sagt: «*Die schnelle Entwicklung und Einführung neuer Technologien, oft nur begleitet von begrenzten Protokollen zur Regelung ihres Benutzers, bringt ihre eigene Risiken mit sich. Die zunehmende Verflechtung von Technologien mit dem grundlegenden Funktionieren von Gesellschaften setzt die Bevölkerung direkten inneren Bedrohungen aus, einschliesslich solcher, die versuchen, das Funktionieren der Gesellschaft zu stören. Parallel zur Zunahme der Cyberkriminalität werden Versuche, kritische Ressourcen und Dienste, die auf Technologien basieren, zu stören, häufiger werden, mit erwarteten Angriffen auf Landwirtschaft und Wasser, Finanzsysteme, öffentliche Sicherheit, Transport, Energie und nationale, Weltraum- und Unterwasser-Kommunikationsinfrastrukturen*».

Sous l'angle spécifique de la cybersécurité, le Global Cybersecurity Outlook 2023 du WEF relève des progrès substantiels par rapport à sa précédente édition en matière de collaboration entre les dirigeants des entreprises interrogées et leur responsables de la cybersécurité. Il révèle toutefois qu'un travail colossal reste à faire pour qu'ils se comprennent, pour exprimer clairement le risque que les cyberproblèmes représentent pour leur entreprise et pour traduire ce risque en mesures de gestion et de réduction effectives. Il pointe aussi le manque de temps restant aux organisations pour développer une cyberrésilience systémique à long terme dans un paysage numérique qui ne cesse de se complexifier. Il insiste sur la priorité qui doit être donnée à l'anticipation plutôt qu'à la réaction et à l'approche stratégique plutôt qu'à la défense tactique. Exactement les messages que nous martelons chez *digi*Volution. Les PME suisses (95% de nos entreprises) sont-elles plus ou moins vertueuses que celles qui ont répondu aux auteurs de ce rapport?

Der WEF Global Cybersecurity Outlook 2023 zeigt im Vergleich zu seiner letzten Ausgabe erhebliche Fortschritte bei der Zusammenarbeit zwischen den Führungskräften der befragten Unternehmen und ihren Cybersicherheitsbeauftragten. Er zeigt jedoch auch, dass noch viel geleistet werden muss, damit sie einander verstehen, das Risiko, das Cyberprobleme für ihr Unternehmen darstellen, klar ausdrücken und dieses Risiko in effektive Management- und Reduktionsmassnahmen umsetzen. Er weist auch darauf hin, dass den Organisationen nicht genügend Zeit bleibt, um in einer immer komplexer werdenden digitalen Landschaft eine langfristige, systemische Cyberresilienz zu entwickeln. Er betont die Priorität, die der Antizipation gegenüber der Reaktion und dem strategischen Ansatz gegenüber der taktischen Verteidigung eingeräumt werden sollte. Das sind genau die Botschaften, die wir bei *digi*Volution vermitteln. Sind die Schweizer KMU (95% unserer Unternehmen) mehr oder weniger tugendhaft als diejenigen, die den Autoren dieses Berichts geantwortet haben?

> Technologies are now shared across a multitude of organizations. These organizations consequently have common dependencies or weaknesses.
>
> *Global Cybersecurity Outlook 2023 – Chapter 1*

► **Les grandes oreilles helvétiques?** – L'article de Republik (premier d'une salve de trois) dénonce un Etat fouineur qui n'aurait tenu aucune de ses promesses de ne pas s'adonner à la surveillance de masse avec la loi sur le renseignement adoptée en 2015. Le procès d'intention fait aux hommes et aux femmes qui, au quotidien, tentent de prévenir les actes criminels et terroristes dirigés contre la Suisse – et aussi de l'intérieur de celle-ci – est pénible à entendre. Il en va de même pour la rhétorique de cet article et de ceux qui lui ont unilatéralement emboîté le pas et qui ne cessent de parler de « services secrets », suggérant par là leur côté soi-disant malsain. Et que dire de l'accusation à peine voilée que nos services

► **Die grossen Ohren der Schweiz?** - Der Artikel in Republik (der erste einer dreier Serie) prangert einen Schnüffelstaat an, der keines seiner Versprechen gehalten habe, mit dem 2015 verabschiedeten Nachrichtendienstgesetz keine Massenüberwachung zu betreiben. Der Vorwurf an die Männer und Frauen, die täglich versuchen, kriminelle und terroristische Handlungen, die gegen die Schweiz – und auch innerhalb der Schweiz – gerichtet sind, zu verhindern, ist schmerzhaft zu hören. Dasselbe gilt für die Rhetorik dieses Artikels und derer, die ihm einseitig gefolgt sind und die ständig von «Geheimdiensten» sprechen und damit deren angeblich bösartige Seite andeuten. Und was ist mit dem kaum

violeraient allégrement les délais d'effacement des données fixés dans l'ordonnance en vigueur depuis 2017 et qui s'attaque ainsi également injustement au personnel de l'Autorité de surveillance indépendante et indirectement au Parlement. Un peu d'objectivité et de respect svp!

► Elections à Taiwan – Malgré le feu roulant de désinformation les visant, les Taïwanais n'ont pas cédé sous la pression persistante de la Chine et élu ce week-end un président défavorable aux exigences chinoises. Tout s'est jusqu'ici passé apparemment sans heurts majeurs. Les Taïwanais ont-ils été plus résilients qu'anticipé? Et ensuite? Les analyses qui suivront fourniront d'utiles piste de réflexions aux Européens et aux Américains pour maîtriser leur propre année électorale. D'autant plus important pour les USA dont la démocratie a été fortement abîmée le 6 janvier 2021. Une longue année en perspective où la fondation DISARM pourrait apporter un début de solution en matière de lutte contre la désinformation.

► Responsabilité des réseaux sociaux – Il y a quelques mois, nous relevions combien le comportement de certains providers était problématique. Il y a eu l'ingérence de Starlink dans la guerre en Ukraine, celle de Facebook dans les incendies de forêt au Canada et les multiples revirements de M. Altman de OpenAI. Un nouveau cas concerne X. Dans le cadre du séisme au Japon, les autorités n'ont pas pu transmettre l'alerte car elles avaient dépassé la quantité de messages gratuits autorisés. Les services japonais n'étaient pas enregistrés en tant que service public ! Combien de personnes ont été mises en danger pour une sombre affaire d'abonnement? Force est de constater que la dépendance de la société face à des services qui ne cessent de changer leurs règles et ne se soucient aucunement de leur responsabilité sociale est incompatible avec la sécurité publique. Conseil à tous les décideurs: avant de confier votre destin et le nôtre à quelqu'un assurez-vous qu'en cas de coup dur vous ne perdiez pas votre souveraineté sur vos fonctions vitales.

verhüllten Vorwurf, dass unsere Dienste, die in der seit 2017 geltenden Verordnung festgelegten Fristen für die Datenlöschung leichtfertig verletzen würden, und der damit auch das Personal der unabhängigen Aufsichtsbehörde und indirekt das Parlament ungerechtfertigt angreift. Ein wenig Objektivität und Respekt, bitte!

► Wahlen in Taiwan – Trotz eines Trommelfeuers von Desinformationen, das auf sie gerichtet ist, haben sich die Taiwaner dem anhaltenden Druck Chinas nicht gebeugt und am Wochenende einen Präsidenten gewählt, der den chinesischen Forderungen nicht nachkommt. Bisher verlief alles weitgehend reibungslos. Waren die Taiwaner resilienter als erwartet? Wie ging es weiter? Die folgenden Analysen werden den Europäern und Amerikanern nützliche Denkanstösse für die Bewältigung ihres eigenen Wahljahres liefern. Dies ist besonders wichtig für die USA, deren Demokratie am 6. Januar 2021 stark beschädigt wurde. Ein langes Jahr liegt vor uns, in dem die DISARM Foundation einen ersten Beitrag zur Bekämpfung von Desinformation leisten könnte.

► Verantwortung sozialer Netzwerke – Vor einigen Monaten wiesen wir darauf hin, dass das Verhalten einiger Anbieter problematisch ist. Es gab die Einmischung von Starlink in den Krieg in der Ukraine, die von Facebook in die Waldbrände in Kanada und die vielen Wendungen von Herrn Altman von OpenAI. Ein neuer Fall betrifft X. Im Zusammenhang mit dem Erdbeben in Japan konnten die Behörden die Warnung nicht weiterleiten, da sie die Menge der erlaubten kostenlosen Messages überschritten hatten. Die japanischen Dienste waren nicht als öffentlicher Dienst registriert! Wie viele Menschen wurden wegen einer dummen Abonnement-Affäre gefährdet? Die Abhängigkeit der Gesellschaft von Diensten, die ihre Regeln ständig ändern und sich nicht um ihre soziale Verantwortung kümmern, ist mit der öffentlichen Sicherheit unvereinbar. Empfehlung an alle Entscheidungsträger: Bevor Sie Ihr und unser Schicksal jemandem anvertrauen, stellen Sie sicher, dass Sie im Falle eines Vorfalles nicht die Souveränität über Ihre lebenswichtigen Funktionen verlieren.

Anticipons sur une tradition chez *digi*Volution, la communication de l'horloge de l'apocalypse / la Doomsday Clock. Ce sera le 23 janvier et vous pourrez le suivre en direct avec ce lien.

Permettez-nous de vous inviter à souscrire à dVPedia Pro et ainsi de soutenir son développement au profit de tous, conformément à la mission que s'est donnée *digi*Volution.

Lassen Sie uns eine Tradition bei *digi*Volution vorwegnehmen, die Bekanntgabe der Doomsday Clock. Sie wird am 23. Januar stattfinden und Sie können sie über diesen Link live verfolgen.

Wir möchten Sie gern weiter dazu einladen, dVPedia Pro zu abonnieren und damit ihre Entwicklung zum Nutzen aller zu unterstützen, ganz im Sinne der Mission von *digi*Volution.

Merci également de soutenir notre travail au profit de la sécurité, de la résilience et de la souveraineté de la Suisse.

Danke auch für die Unterstützung unserer Arbeit zur Förderung der Sicherheit, Resilienz und Souveränität der Schweiz.

digiVolution

TWINT

Nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés et vous retrouverons dans 15 jours.

Wir wünschen Ihnen viele lehrreiche Entdeckungen bei den ausgewählten Artikeln und Links und sehen uns in zwei Wochen wieder.

[i] *Depuis le 8 janvier 2021, digiVolution publie un billet de réflexion (newsletter) qui accompagne une sélection d'articles « hand picked » pour illustrer la complexité des défis liés à la mutation digitale ; ils sont disponibles à l'adresse https://www.digivolution.swiss/dv-blog. Les personnes intéressées trouveront sur cette même page le lien pour s'y inscrire. /// Seit dem 8. Januar 2021 veröffentlicht digiVolution regelmässig einen Newsletter, der von einer Auswahl «handverlesener» Artikel begleitet wird, die die Komplexität, der mit der digitalen Mutation verbundenen Herausforderungen veranschaulichen; Sie finden diese unter https://www.digivolution.swiss/dv-blog. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.*