Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[26.10.2023 – Édition / Ausgabe Nr. 87]

Strategic surprise

Chers Lectrices et Lecteurs

Voici les *d*V-News 21-2023 et leur sélection d'articles et liens.

Jour d'élection - À l'heure où s'écrivent ces lignes, les Suisses viennent d'élire leur Parlement. Chez *digi*Volution, nous nous engagerons également pour qu'une **politique de numérisation sûre** figure parmi les priorités de la nouvelle assemblée, la sécurité étant un besoin essentiel de notre « société de la donnée ». L'article de René Jaun de la Netzwoche montre combien le gouffre que la Suisse **DOIT** franchir est large, comme l'attestent d'ailleurs les chiffres que nous répétons à chacun de nos billets bihebdomadaires. Le danger d'un décrochage technologique de notre pays ou de conséquences sécuritaires insupportables en cas de cyberévénement majeur **DOIT** être pris au sérieux. Au seuil de la nouvelle législature, nous constatons que le programme des partis politiques en matière de numérisation et de cybersécurité est quasi inexistant et seuls quelques candidats s'en préoccupent. Il y a donc beaucoup à faire et *digi*Volution fera sa part durant les quatre ans. Car **la Suisse dépend de façon systémique d'une numérisation performante et sûre**. Ne pas prendre ce domaine au sérieux – donc y investir lourdement – **c'est risquer de se retrouver confronté à une surprise stratégique**. L'exemple d'Israël le 7 octobre dernier doit nous alarmer. Il démontre une fois encore que **la connaissance est la première ligne de défense contre la surprise**. Et c'est exactement dans cette optique qu'a aussi été créé *d*VPedia.

Liebe Leserinnen und Leser

Hier sind die *d*V-News 21-2023 und eine Auswahl an Artikeln und Links.

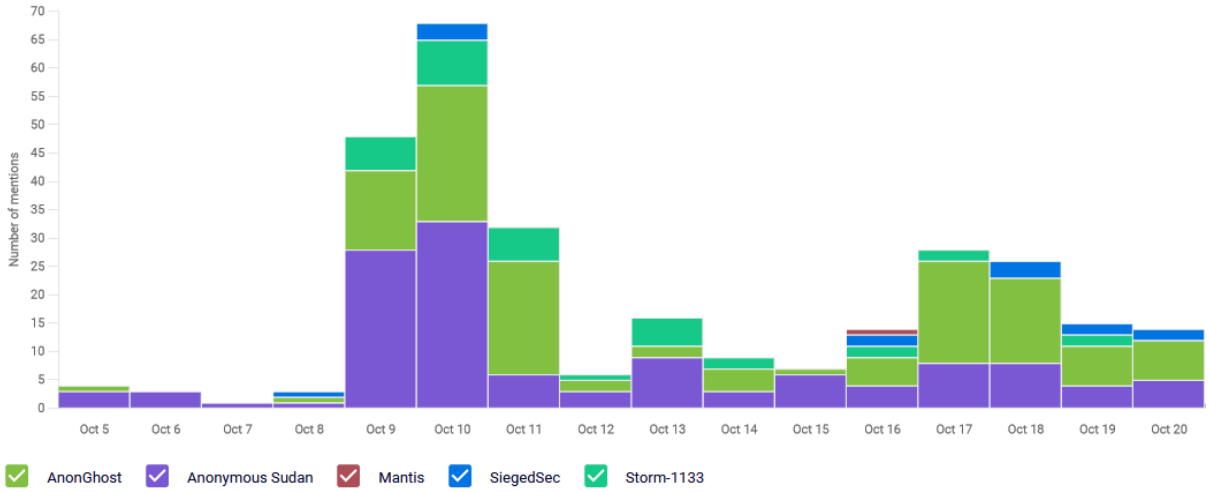
Wahltag - Während diese Zeilen geschrieben werden, haben die Schweizerinnen und Schweizer ihr Parlament gewählt. Wir setzen uns bei *digi*Volution dafür ein, dass eine **sichere Digitalisierungspolitik** zu den Prioritäten des neuen Parlaments gehört, da Sicherheit ein Grundbedürfnis unserer «Datengesellschaft» ist. Der Artikel von René Jaun in der Netzwoche zeigt, wie gross die Kluft ist, die die Schweiz überbrücken **MUSS**. Dies belegen übrigens auch die Zahlen, die wir in jedem unserer zweiwöchentlich erscheinenden Beiträge aufzeigen. Die Gefahr eines technologischen Rückstands unseres Landes oder von untragbaren Sicherheitsfolgen im Falle eines grossen Cybereregnisses **MUSS** ernst genommen werden. An der Schwelle zur neuen Legislaturperiode stellen wir fest, dass die politischen Parteien kaum Programme zur Digitalisierung und Cybersicherheit vorlegen und nur wenige Kandidaten sich darum kümmern. Es gibt also viel zu tun, und *digi*Volution wird in den nächsten vier Jahren seinen Teil dazu beitragen. Denn **die Schweiz ist systemisch von einer leistungsfähigen und sicheren Digitalisierung abhängig**. Wer diesen Bereich nicht ernst nimmt – und entsprechend viel investiert – **riskiert, mit einer strategischen Überraschung konfrontiert zu werden**. Das Beispiel Israels am 7. Oktober soll uns alarmieren. Es zeigt wieder einmal, dass **Wissen die erste Verteidigungslinie gegen Überraschungen ist**. Und genau zu diesem weck wurde auch *d*VPedia entwickelt.

Israël – Chez *digi*Volution nous sommes profondément choqués par le déluge de violence qui s'est abattu sur Israël. Rien ne justifie la barbarie perpétrée le 7 octobre. C'est intolérable, de portée historique et rappelle des heures très sombres du XXe siècle. Mais peut-être le pire est-il bien l'objectif des terroristes du Hamas et de ses sponsors. L'Histoire jugera.

Avec l'outil PEEK de LinkAlong, nous avons réalisé une première analyse des événements de ce conflit dans le cyberespace entre le 1er et le 20 octobre. Une fois de plus nous avons vérifié combien la dimension cyber fait partie de la guerre et les centaines d'articles mis en évidence ont rapidement livré l'identité des acteurs de la menace.

Israel - Wir sind bei *digi*Volution zutiefst schockiert über die Sintflut der Gewalt, die über Israel hereingebrochen ist. Es gibt keine Rechtfertigung für die Barbarei, die am 7. Oktober verübt wurde. Das ist unerträglich, von historischer Tragweite und erinnert an sehr dunkle Stunden des 20. Jahrhunderts. Aber vielleicht ist das Schlimmste tatsächlich das Ziel der Hamas-Terroristen und ihrer Sponsoren. Die Geschichte wird darüber urteilen.

Mit dem PEEK-Tool unseres Partners LinkAlong haben wir eine erste Analyse der Ereignisse dieses Konflikts im Cyberraum zwischen dem 1. und dem 20. Oktober durchgeführt. Erneut hat sich gezeigt, wie gross die Cyberdimension Teil des Krieges ist, und Hunderte von signifikanten Artikeln lieferten rasch die Identität der Akteure der Cyberbedrohung.

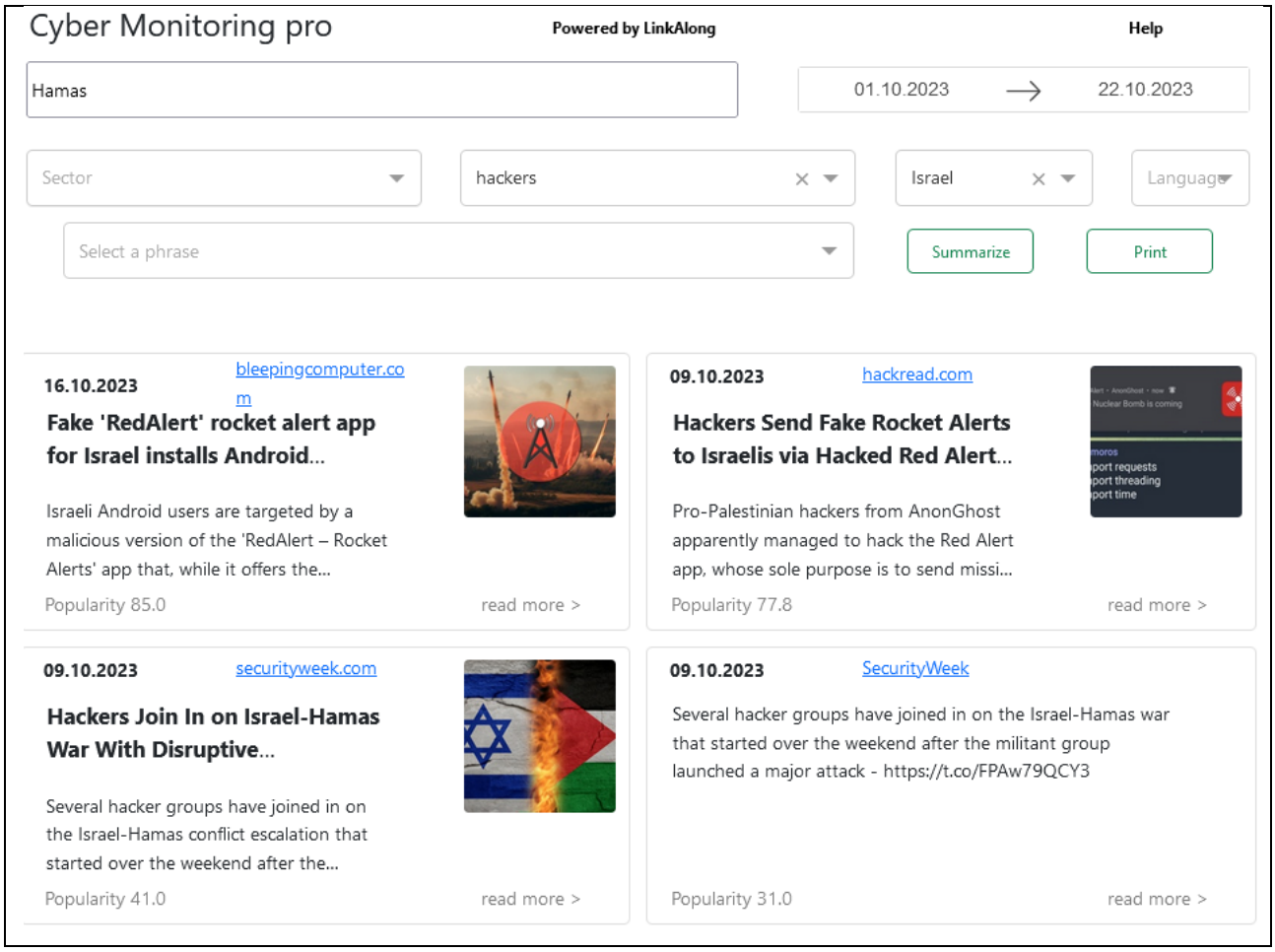


L'analyse a ainsi rapidement révélé l'existence de 58 groupes impliqués dans des cyberattaques, 10 en soutien à Israël et 48 au profit des Palestiniens.

Avec dVPedia nous avons ensuite interrogé *d*VTopics selon le masque de saisie ci-dessous. En quelques secondes nous avons obtenu 112 informations significatives classées par popularité.

Die Analyse ergab rasch, dass 58 Gruppen an Cyberattacken beteiligt waren, 10 zur Unterstützung Israels und 48 zugunsten der Palästinenser.

Bei dVPedia haben wir dann *d*VTopics gemäss der untenstehenden Eingabemaske abgefragt. Innerhalb weniger Sekunden erhielten wir 112 relevante Informationen, nach Popularität geordnet.



Avec l'option « *Summarize* », nous avons ensuite obtenu le résumé des huit nouvelles les plus discutées et le lien vers ces références.

Mit der Option «*Summarize*» erhielten wir anschliessend die Zusammenfassung der acht am meisten diskutierten Nachrichten und den Link zu diesen Referenzen.

In recent news, cyberattacks have been rampant in the ongoing conflict between Israel and Gaza. A Gaza-based threat actor named Storm-1133 has been targeting Israeli energy, defense, and telecommunications organizations using tactics such as social engineering, fake LinkedIn profiles, and phishing messages [1]. Additionally, hackers have been distributing a malicious version of the 'RedAlert - Rocket Alerts' app to Israeli Android users, posing as a legitimate tool while secretly collecting and uploading user data [2]. Pro-Palestinian hackers from AnonGhost have also conducted a cyberattack on the RedAlert app, sending false missile and bomb alerts to Israeli users, further escalating the conflict [3]. Israel's government and media websites have not been spared either, as they have also been hit by cyberattacks during the gun battles [4]. Hacktivist groups from both sides have intensified their cyberattacks, including groups like Killnet [5][6][7]. These events highlight the limitations of even advanced surveillance software, such as NSO Group's Pegasus, in providing advance warnings of cyberattacks [8].

References

[1] Gaza-Linked Cyber Threat Actor Targets Israeli Energy and Defense Sectors, thehackernews.com

[2] Fake 'RedAlert' rocket alert app for Israel installs Android spyware, bleepingcomputer.com

[3] Hackers Send Fake Rocket Alerts to Israelis via Hacked Red Alert App, hackread.com

[4] Israel's government, media websites hit with cyberattacks. The gun battles between Hamas and the Is..., Anonymous Link
[5] Hackers Join In on Israel-Hamas War With Disruptive Cyberattacks, securityweek.com
[6] Several hacker groups have joined in on the Israel-Hamas war that started over the weekend after the..., SecurityWeek
[7] Israel's government, media websites hit with cyberattacks. Hacktivists, including cyber gangs such a..., CyberNews
[8] Why Israel's Pegasus spyware was not enough to stop Hamas, cyberguy.com

Le résultat parle de lui-même. Il n'y a rien à ajouter. Un nouveau front s'est ouvert qui occulte déjà la guerre en Ukraine. L'actualité chasse l'actualité et les projecteurs sont désormais braqués ailleurs. Pour tous les responsables de sécurité, il s'agit donc de veiller à ce que les acteurs malveillants ne profitent pas de «*l'effet tunnel*» provoqué par la sidération née de ces tragiques événements. Et l'incendie est loin d'être éteint…!

Das Ergebnis spricht für sich selbst. Es gibt nichts mehr hinzuzufügen. Es wurde eine neue Front eröffnet, die den Krieg in der Ukraine bereits in den Hintergrund gedrängt hat. Die Nachrichten vertreiben die Nachrichten und die Scheinwerfer sind nun auf andere Bereiche gerichtet. Für alle Sicherheitsverantwortlichen gilt es nun, dafür zu sorgen, dass böswillige Akteure nicht den «*Tunnel-Effekt*» ausnutzen, der durch die Verblüffung über diese tragischen Ereignisse ausgelöst wurde. Und das Feuer ist noch lange nicht gelöscht...!

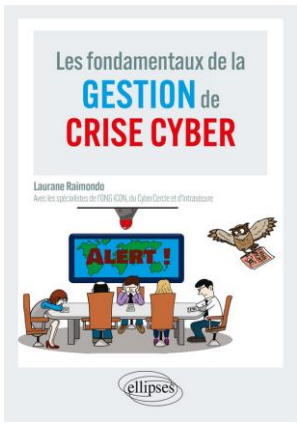
Permettons-nous, en ces heures sombres, de rappeler que tout abonné à *d*VPedia Pro peut, sur toute question en lien avec des cyberincidents, n'importe quand et à l'échelle mondiale, interroger notre base de connaissance et produire de tels résultats. C'est unique!

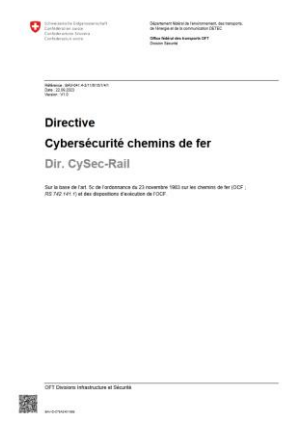
In diesen dunklen Stunden möchten wir doch aufmerksam machen, dass *d*VPedia-Pro-Abonnenten jederzeit und weltweit unsere Wissensdatenbank zu Fragen im Zusammenhang mit Cybervorfällen abfragen und Ergebnisse liefern können. Es ist einzigartig!

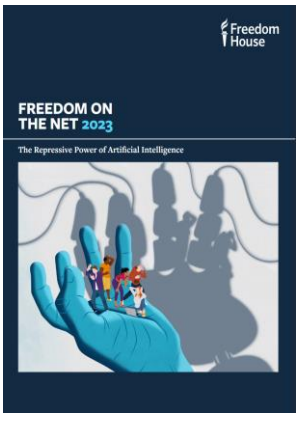
BOOKS & REPORTS

Voici les livres et publications d'intérêts découverts durant nos recherches des dernières deux semaines. Pour rappel, ne souhaitant pas faire de la promotion pour quelques éditeurs que ce soit quand il s'agit d'ouvrages commerciaux, nous vous laissons trouver le distributeur qui vous convient.

Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in den letzten zwei Wochen gefunden haben. Wir möchten Sie daran erinnern, dass wir bei kommerziellen Büchern nicht für einen Verlag werben und überlassen es Ihnen, den für Sie passenden Händler zu finden.







En bref, quelques autres nouvelles qui ont retenu notre attention durant les deux semaines écoulées.

- **Microsoft Digital Defense Report** – S'agissant de la Suisse, ce rapport montre trois éléments intéressants. ▶ La patrie de Heidy est une des cibles européennes privilégiées des hackers nord-coréens. ▶ Avec 14% de femmes actives dans la cybersécurité, la Suisse est un des pays où la disparité hommes-femmes reste la plus élevée. ▶ En Europe, la Suisse est un des pays les plus visés par les acteurs de la menace, à parité avec l'Allemagne. Dans notre billet nr. 84 du 12 septembre, nous citions l'étude du

In Kürze, einige weitere Themen, die uns in den vergangenen zwei Wochen besonders beschäftigten.

- **Microsoft Digital Defense Report** – In Bezug auf die Schweiz zeigt dieser Bericht drei interessante Elemente. ▶ Heidyland ist eines der bevorzugten europäischen Ziele für nordkoreanische Hacker. ▶ Mit 14% Frauenanteil im Bereich Cybersicherheit ist die Schweiz eines der Länder, in denen das Geschlechtergefälle immer noch am grössten ist. ▶ In Europa ist die Schweiz eines der Länder, die von den Bedrohungsakteuren am häufigsten ins Visier genommen werden, gleichauf mit Deutschland. In unserem

BITKOM allemand et le coût de 3.8% que les cyberattaques seules pèsent sur l'économie allemande. Cela signifierait pour la Suisse qui selon Microsoft est pareillement touchée, une facture de près de 30 milliards, soit près de 6 fois le budget de l'armée. **Et la Suisse ne perçoit toujours pas cette urgence absolue?**

- **Vous avez aimé PEGASUS ? Vous allez adorer PREDATOR** – Encore un outil d'attaque et de surveillance – européen cette fois - basé sur des failles de sécurité dans les systèmes d'exploitation et les logiciels populaires de nos **smartphones. Aucun n'est immunisé**. La Suisse en fait-elle usage? L'enquête à laquelle ont notamment participé Der Spiegel, Mediapart et Amnesty International mène également dans notre pays. Après avoir insisté, la Wochenzeitung a appris que Fedpol s'y est intéressée, mais semble-t-il sans suite. Ce qui est important c'est qu'une fois encore il est ainsi démontré, qu'**aucune conversation classifiée ne doit avoir lieu à proximité ou avec un smartphone**. Est-ce que les applications populaires de sécurité apportent tout de même une certaine protection? Des tests exhaustifs sont nécessaires, mais dans l'intervalle, les personnes et entreprises à risques feraient mieux de s'abstenir. Début octobre, le Washington Post a rapporté que plusieurs membres du Congrès américain, des membres de groupes de réflexion sur l'Asie et des journalistes, ont été ciblés au travers de liens infectés envoyés via X (anciennement Twitter). A la manœuvre, le gouvernement vietnamien!
- **5G –** Rappelons que la Suisse est à la traîne, mais le Parlement a enfin adopté une motion chargeant le Conseil fédéral de prendre les mesures et les décisions nécessaires pour avancer avec le déploiement de la 5G tout en fournissant au grand public toutes les informations pertinentes. Mais on aura à peine terminé ce débat que déjà il sera question de la 6G. Il serait urgent que le

Newsletter Nr. 84 vom 12. September zitierten wir die Studie des deutschen BITKOM und die Kosten von 3,8% des BIP, die allein durch Cyberangriffe auf die deutsche Wirtschaft entstehen. Für die Schweiz, die laut Microsoft ebenso stark betroffen ist, würde dies eine Rechnung von fast CHF 30 Milliarden bedeuten, was fast dem Sechsfachen des Armeebudgets entspricht. **Und die Schweiz sieht diese absolute Dringlichkeit immer noch nicht?**

- **Hat Ihnen PEGASUS gefallen? Dann werden Sie PREDATOR lieben** – Ein weiteres - diesmal europäisches - Angriffs- und Überwachungswerkzeug, das auf Sicherheitslücken in den beliebten Betriebssystemen und Softwareprogrammen unserer **Smartphones basiert. Keines davon ist immun**. Macht die Schweiz davon Gebrauch? Die Untersuchung, an der unter anderem Der Spiegel, Mediapart und Amnesty International beteiligt waren, führt auch in unser Land. Die Wochenzeitung hat auf Nachfrage erfahren, dass Fedpol sich dafür interessiert hat, aber offenbar nichts weiter unternommen hat. Wichtig ist, dass damit wieder einmal gezeigt wird, dass **keine klassifizierten Gespräche in der Nähe oder mit einem Smartphone stattfinden dürfen**. Bieten populäre Sicherheitsanwendungen dennoch einen gewissen Schutz? Breite Tests sind notwendig, aber bis dahin sollten Personen und Unternehmen bei riskanten Themen oder Kontakten lieber die Finger davon lassen. Anfang Oktober berichtete die Washington Post, dass mehrere Mitglieder des US-Kongresses, Mitglieder asiatischer Denkfabriken und Journalisten über infizierte Links, die über X (früher Twitter) versendet wurden, ins Visier genommen wurden. Dahinter steckt die vietnamesische Regierung!
- **5G** – Die Schweiz hinkt hinterher, aber das Parlament hat endlich einen Antrag angenommen, der den Bundesrat beauftragt, die notwendigen Massnahmen und Entscheidungen zu treffen, um die Einführung von 5G voranzutreiben und gleichzeitig die

Parlement adopte un rythme en rapport avec celui de la technologie…!

- **Quantum** – Annoncé lors de la conférence annuelle du GESDA en 2022, le Open Quantum Institute est désormais bien né. Face aux enjeux très importants que représente cette technologie, il s'agit là d'une avancée importante qui mettra la Suisse au centre de l'agenda international. Mais quid de la protection contre la puissance de calcul de cette technologie qui mettra en péril toutes les formes de cryptographie qui protègent notre confidentialité?
- **Tempêtes solaires** – Nous rapportons régulièrement que la prochaine grosse tempête solaire devrait se passer en juillet 2025. Et notre dernier billet commentait les aurores boréales inhabituelles observées jusqu'en Suisse le 25 septembre dernier. De récentes observations dans des bois fossilisés ont permis de découvrir près de 8 tempêtes. Ces «événements de Miyake», y compris la tempête vieille de 14300 ans récemment découverte, «auraient été d'un ordre de grandeur stupéfiant». Elles causeraient aujourd'hui des dégâts sans précédent et reléguerait l'événement de Carrington de 1859, le plus intense observé à ce jour, au rang de hors-d'œuvre. Qui se soucie de ce danger?
- **Environnement** – Un bon point pour la digitalisation qui permettrait à l'Allemagne d'économiser 163 millions de tonnes de CO2 d'ici à 2050, soit 20% de ses émissions totales. Un mauvais point cependant pour l'IA : la consommation de Google en 2021 s'est élevée à 18,3 térawattheures (TWh), une facture qui pourrait être comprise entre 85 et 134 TWh d'ici à 2027 à cause de l'IA. Pour comparer: en 2022 la Suisse a consommé 57 TWh.

Öffentlichkeit mit allen relevanten Informationen zu versorgen. Kaum wird aber diese Debatte beendet sein, wird bereits 6G Realität sein. Es wäre dringend notwendig, dass das Parlament ein Tempo einschlägt, das mit dem der Technologie Schritt hält...!

- **Quantum** – Das Open Quantum Institute wurde auf der GESDA-Jahreskonferenz 2022 angekündigt und ist nun geboren. Angesichts der grossen Herausforderungen, die diese Technologie mit sich bringt, ist dies ein wichtiger Schritt, der die Schweiz in den Mittelpunkt der internationalen Agenda rücken wird. Aber was ist mit dem Schutz vor der Rechenleistung dieser Technologie, die alle Formen der Verschlüsselung, die unsere Vertraulichkeit schützen, gefährden wird?
- **Sonnenstürme** – Wir berichten regelmässig, dass der nächste grosse Sonnensturm im Juli 2025 stattfinden könnte. Und in unserem letzten Newsletter kommentierten wir die ungewöhnlichen Nordlichter, die am 25. September bis in die Schweiz beobachtet wurden. Neueste Beobachtungen in versteinertem Holz haben fast acht Stürme aufgedeckt. Diese «Miyake-Ereignisse», einschliesslich des kürzlich entdeckten 14300 Jahre alten Sturms, «wären in einer atemberaubenden Grössenordnung gewesen». Sie würden heute noch nie dagewesene Schäden verursachen und das Carrington-Ereignis von 1859, das bislang stärkste beobachtete Ereignis, in den Hintergrund drängen. Wer kümmert sich um diese Gefahr?
- **Umwelt** – Ein positiver Punkt für die Digitalisierung ist, dass sie es Deutschland ermöglichen würde, bis 2050 163 Milliarden Tonnen CO2 einzusparen, was 20% seiner Gesamtemissionen entspricht. Ein negativer Punkt allerdings erhält die KI: Google verbrauchte 2021 18,3 Terawattstunden (TWh), eine Rechnung, die aufgrund der KI bis 2027 auf 85 bis 134 TWh ansteigen könnte. Zum Vergleich: Im Jahr 2022 verbrauchte die Schweiz 57 TWh.

Nous souhaitions changer la formule de notre billet bihebdomadaire lors de cette édition. Les événements en Israël nous ont momentanément détournés de notre objectif. Mais ça vient.

D'ici là nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés et nous réjouissons de vous retrouver bientôt.

Wir wollten eigentlich in dieser Ausgabe das Format unseres zweiwöchentlichen Beitrags ändern. Die Ereignisse in Israel haben uns jedoch von diesem Vorhaben momentan abgehalten. Das kommt noch.

Bis dahin wünschen wir Ihnen viele lehrreiche Entdeckungen bei den ausgewählten Artikeln und Links und freuen uns, Sie bald wieder zu informieren.

Vous souhaitez soutenir l'action de *digi*Volution? Écrivez-nous /// Möchten Sie die Arbeit von *digi*Volution unterstützen? Schreiben Sie uns an info@digivolution.swiss

[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.*