

Les billetsⁱ de *digiVolution* / *digiVolution's* Newsletters
[23.05.2023 – Édition / Ausgabe Nr. 76]

Cyber Attrition

Chers Lectrices et Lecteurs

Voici les **dV-News 10-2023** et leur sélection d'[articles et liens](#) et une réflexion sur la manière de se protéger contre le fléau toujours plus incontrôlable des défis sécuritaires de la mutation numérique.

Sortir de la logique de cyber attrition

Osons une discussion provocatrice... Y a-t-il une autre voie possible que le combat de coqs sur leur tas de fumier? L'image est certes osée, mais force est de constater que nous sommes dans une situation insoluble qui va inexorablement à l'échec.

Tout d'abord nous sommes dans une situation de dissymétrie par rapport à nos concurrents et adversaires. Nos forces sont qualitativement comparables, mais quantitativement très inférieures et à la fin c'est toujours le plus gros qui gagne. Ce n'est qu'une question de temps. On peut prendre toutes les mesures imaginables, l'expérience montre que les cyberagresseurs s'adaptent rapidement et savent souvent mieux faire usage des nouvelles technologies que les défenseurs. Nous sommes aussi dans une situation d'asymétrie, car nous ne nous battons pas sur le même plan. Les défenseurs sont les seuls à s'en tenir aux règles et les agresseurs savent ce que la défense peut ou ne peut pas faire. Ils savent aussi que les *mieux-sachants* vont les [désavouer](#) dès qu'ils franchiront les lignes que seule notre infinie naïveté a créé.

Les chiffres publiés en début d'année par [STATISTA](#) montrent que les dégâts de la cybercriminalité à l'échelle mondiale passeront de

Liebe Leserinnen und Leser

Dies sind die **dV-News 10-2023** und eine Auswahl an [Artikel und Links](#) und einer Reflexion darüber, wie man sich vor der zunehmend unkontrollierbaren Bedrohungen der Sicherheits Herausforderungen des digitalen Wandels schützen kann.

Die Vorstellung einer Cyber-Zerschlagung vergessen

Lassen Sie uns eine provokative Diskussion riskieren... Gibt es einen anderen Weg als den Kampf der Hähne auf ihrem Misthaufen? Es ist ein gewagtes Bild, aber wir müssen feststellen, dass wir uns in einer unlösbaren Situation befinden, die unweigerlich zum Scheitern führt.

Zuerst einmal stehen wir im Vergleich zu unseren Mitbewerbern und Gegnern in einer dissymmetrischen Position. Unsere Stärken sind qualitativ vergleichbar, aber quantitativ weit unterlegen, und am Ende gewinnt immer der Grösste. Es ist nur eine Frage der Zeit. Man kann alle erdenklichen Massnahmen ergreifen, aber die Erfahrung zeigt, dass Cyberangreifer sich schnell anpassen und neue Technologien oft besser nutzen als Verteidiger. Wir befinden uns auch in einer asymmetrischen Situation, weil wir uns nicht auf der gleichen Ebene bewegen. Die Verteidiger sind die einzigen, die sich an die Regeln halten, und die Angreifer wissen, was sie tun können und was nicht. Sie wissen auch, dass die *Besserwisser* sie [desavouieren](#) werden, sobald sie die Grenzen überschreiten, die wir



8'440 milliards de dollars US en 2022 à 23'820 milliards de dollars US en 2027 (soit près d'un quart de la richesse mondiale produite...). Ce sont probablement des chiffres très pessimistes, mais ils sont l'expression d'une réalité, en [Suisse](#) aussi et malgré les investissements continus consacrés à la cybersécurité. C'est comme tenter d'écoper un bateau qui prend toujours plus d'eau avec un seau trop petit. À la fin il y a quand même naufrage. Le NCSC et l'industrie suisse de la cybersécurité font un boulot remarquable, ils sont souvent à la pointe de l'innovation technique et les [forces de l'ordre](#) internationales démantèlent régulièrement des gangs criminels, rien n'y fait, la casse augmente inexorablement. Parfois même les malwares sont encore [implantés déjà lors de la fabrication des produits](#)... ! À ce train-là, les dégâts vont devenir insupportables. Peut-on espérer un changement de tendance? Les neuf thèses sectorielles ci-dessous (chez [digiVolution](#) nous suivons 25 domaines) tendent à dire le contraire.

allerdings nur unserer unendlichen Naivität zu verdanken haben.

Die zu Jahresbeginn von [STATISTA](#) veröffentlichten Zahlen zeigen, dass der weltweite Schaden durch Cyberkriminalität von 8'440 Milliarden US-Dollar im Jahr 2022 auf 23'820 Milliarden US-Dollar in 2027 ansteigen wird (somit fast ein Viertel des weltweit produzierten Bruttosozialprodukts...). Dies sind wahrlich sehr pessimistische Zahlen, aber sie sind Ausdruck der Realität, auch in der [Schweiz](#) und trotz anhaltender Investitionen in die Cybersicherheit. Es ist, als würde man versuchen, ein Boot, das immer mehr Wasser leckt, mit einem zu kleinen Eimer zu auszuschöpfen. Am Ende kentert es doch noch. Das NCSC und die Schweizer Cybersicherheitsindustrie machen einen bemerkenswerten Job, sie sind oft auf der Höhe der technologischen Innovation und internationale [Polizeikräfte](#) zerschlagen regelmässig kriminelle Banden, aber es hilft nichts, der Schaden steigt unaufhaltsam. Manchmal werden sogar [Schadsoftware bereits bei der Produktherstellung](#) implantiert...! Wenn es so weitergeht, wird der Schaden unerträglich werden. Kann man auf einen Trendwechsel hoffen? Die folgenden neun branchenspezifischen Thesen (bei [digiVolution](#) verfolgen wir 25 Branchen) besagen das Gegenteil.

Geopolitics The increasing number and severity of armed and unarmed inter-state conflicts brings us into a zone of great uncertainty	Cyber exposure The complexity and the attack surface make cyberspace more and more impossible to protect with intolerable systemic damage	Dependencies As COVID brutally exposed, we are dependent on uncontrollable supply chains without credible plan B in the face of our growing loss of sovereignty
Logic of blocks We are living the rebirth of a world separated by deep rifts challenging and destroying the World Order inherited from WWII	Digital control The immaturity of the digital society, her lack of knowledge and insufficient means to impose her choices leave all powers to the service providers	Trust Everyone talks about it, but we just have to admit that on a global scale, this societal (and not only technical) value is rapidly declining
Technology Pseudo-moratoriums on AI and heterogeneous legal frameworks that always lag behind technology and business are unlikely to change anything	Ageing society In 2030, 1/3 of the Swiss population will be over 65 years old and it will become increasingly difficult to educate them about cyber risks	Scarcity of manpower How to compensate for the talent shortage that is affecting all sectors and is getting worse due to the ubiquity and increasing demand for ICT?



Comme l'a exposé le chef d'état-major français des armées, le contexte géostratégique est sorti du continuum classique de *paix - crise - guerre* pour entrer dans une boucle de *compétition - contestation - affrontement*. Le monde se trouve ainsi bien plus souvent dans une situation conflictuelle qui ne dit pas son nom, mais qui est bien réelle à tous les niveaux en termes de pertes de pouvoir, de souveraineté, de marchés, etc. avec de nouveaux modes opératoires, où se mélangent intimidation stratégique, ambiguïté, violence, etc.

Dans ce contexte, les thèses exposées ci-dessus - et on ne parle même pas de la question énergétique qui va revenir - montrent que l'eau monte inexorablement dans la cale du navire. Bien entendu il faut continuer à écoper pour ralentir le naufrage, mais cela ne suffira pas, nous le savons déjà. Alors que faire face à son inexorable occurrence?

La réponse n'est de loin pas simplement *plus de technologie, plus de cybersécurité* ou *plus de régulation*. C'est à trouver des réponses que nous travaillons chez *digiVolution* et nous invitons toutes les bonnes volontés et ceux qui ont compris les enjeux à soutenir notre action.

[CONTACTEZ-NOUS !](#)

Nach Einschätzung des französischen Generalstabschefs hat der geostrategische Kontext das klassische Kontinuum von *Frieden - Krise - Krieg* verlassen und ist in eine Schleife von *Wettbewerb - Herausforderung - Konfrontation* eingetreten. Die Welt befindet sich daher viel häufiger in einer Konfliktsituation, die zwar so nicht genannt wird, aber auf allen Ebenen sehr real ist, was den Verlust von Macht, Souveränität, Märkten usw. angeht, mit neuen Vorgehensweisen, in denen sich strategische Einschüchterung, Mehrdeutigkeit, Gewalt usw. vermischen.

In diesem Rahmen, die oben genannten Thesen - und wir sprechen dabei noch nicht von der Energiefrage, die wieder aufkommen wird - zeigen, dass das Wasser im Schiff unaufhaltsam steigt. Natürlich müssen wir weiter schöpfen, um den Untergang zu verlangsamen, aber das wird nicht ausreichen, wie wir bereits wissen. Was sollen wir angesichts seines unaufhaltsamen Kenterns tun?

Die Antwort ist bei weitem nicht einfach *mehr Technologie, mehr Cybersicherheit* oder *mehr Regulierung*. Wir bei *digiVolution* arbeiten daran, Antworten darauf zu finden, und laden alle Gutgesinnten und diejenigen die verstanden haben, was auf dem Spiel steht, dazu ein, unsere Arbeit zu unterstützen.

[NIMM KONTAKT MIT UNS AUF!](#)



Image générée par DALLE-E d'un « groupe réfléchissant à des solutions pour affronter les cybermenaces » // Von DALLE-E erstelltes Bild einer «Gruppe, die über Lösungen für den Umgang mit Cyberbedrohungen nachdenkt».



Cyberactualité

Les sujets clés qui ont retenu notre attention durant les deux semaines écoulées.

- **Souveraineté numérique** - La discussion en Suisse se poursuit malgré la passivité de Berne et cela est réjouissant. L'initiative des [cantons latins](#) fait particulièrement plaisir avec une définition du terme «*souveraineté*» de bon niveau : «*la capacité des autorités à maintenir leur autonomie stratégique, soit à pouvoir utiliser et contrôler de manière autonome les biens matériels et immatériels et les services numériques qui impactent l'économie, la société et la démocratie*». Nous aurions souhaité que le mot «*autorités*» cède sa place à «*entité*», car tout le monde est concerné, de l'individu à l'État, mais c'est là déjà un pas très positif. Une initiative de [l'association Innovate Switzerland](#) traite du même sujet, mais là notre enthousiasme est beaucoup plus mesuré, car le but annoncé est «*promouvoir une utilisation responsable des données et de la technologie de cloud public en Suisse et renforcer la capacité d'innovation du pays*». En fait, ce texte est vide de toute idée de souveraineté et la composition du comité qui en est l'auteur laisse penser que les enseignements du fiasco de [Gaia-X](#), le projet de cloud européen qui a commencé à capoter avec l'arrivée des GAFAM, n'ont pas été tirés.
- **Nouvelle loi sur la protection des données nLPD** - Le Préposé fédéral à la protection des données et à la transparence (PFPDT) a publié une [explication générale](#) sur la nouvelle loi. Mais à 3.5 mois de son entrée en vigueur, il n'y a toujours aucune réponse quant à l'équivalence de la nLPD avec le RGPD européen (l'UE n'est-elle pas notre principal partenaire économique ?) ni aucune aide concrète quant à des marches à suivre, recommandations concrètes, formulaires d'aide, etc. C'est léger ! Mais les émoluments sont définis ! Pourtant face à [l'explosion d'applications d'IA](#) qui compliquent chaque jour la gestion des

Cyberaktualität

Die Schlüsselthemen, die uns in den vergangenen zwei Wochen beschäftigten.

- **Digitale Souveränität** - Die Diskussion in der Schweiz geht trotz der Passivität von Bern weiter und das ist erfreulich. Besonders erfreulich ist die Initiative der [lateinischen Kantone](#) mit einer guten Definition des Begriffs «*Souveränität*»: «*Die Fähigkeit der Behörden, ihre strategische Autonomie zu bewahren, d.h. materielle und immaterielle Güter und digitale Dienste, die Wirtschaft, Gesellschaft und Demokratie beeinflussen, autonom zu nutzen und zu kontrollieren*». Wir würden es begrüßen, wenn das Wort «*Behörden*» durch «*Instanzen*» ersetzt würde, da alle betroffen sind, vom Einzelnen bis zum Staat, aber dies ist bereits ein sehr positiver Schritt. Eine Initiative des [Vereins Innovate Switzerland](#) behandelt auch dieses Thema, aber hier ist unsere Begeisterung viel gedämpfter, da das erklärte Ziel darin besteht, «*eine verantwortungsvolle Nutzung von Daten und Public-Cloud-Technologie in der Schweiz zu fördern und die Innovationsfähigkeit des Landes zu stärken*». Hier fehlt jegliche Idee von Souveränität und die Zusammensetzung des Komitees, das den Text verfasst hat, lässt vermuten, dass die Lehren aus dem Fiasco von [Gaia-X](#), dem europäischen Cloud-Projekt, das mit der Ankunft der GAFAMs zu kollabieren begann, nicht gezogen wurden.
- **Neues Datenschutzgesetz nDSG** - Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) hat eine [allgemeine Erklärung](#) zum neuen Gesetz veröffentlicht. Aber 3,5 Monate vor Inkrafttreten des Gesetzes gibt es immer noch keine Antwort auf die Frage, ob das nDSG mit der europäischen DSGVO gleichwertig ist (ist die EU nicht unser wichtigster Wirtschaftspartner?), und es gibt immer noch keine konkrete Hilfe in Form von Vorgehensweisen, konkreten Empfehlungen, Hilfsformularen, etc. Fahrlässig! Aber die Gebühren sind festgelegt! Doch angesichts der



données, les entreprises et institutions auraient bien besoin de quelques outils.

- **L'Europe en bref** - ▶ Le [cloud souverain](#), pourrait devenir l'Arlésienne 4.0. ▶ Le Data Act fait face à des [vents contraires](#), les entreprises craignant pour leur compétitivité. ▶ Il nous faudra apprendre un nouvel acronyme : [ECCC](#) pour l'*European Cybersecurity Competence Centre and Network* qui vient d'être inauguré à Bucarest. Espérons que l'activité de ce centre se distinguera bien des entités nationales, de l'[ENISA](#), du [CCDCOE](#) ou encore du [Hybrid CoE](#) et apportera une véritable plus-value. ▶ Prenons enfin connaissance du [manifeste de la JEDI](#) - *Joint European Disruptive Initiative* qui veut fédérer les États européens autour d'une initiative de type [DARPA](#) pour ramener le continent parmi les puissances technologiques, notamment au moyen d'une gouvernance agile, loin des standards européens inefficaces et autour d'un nombre limité de thèmes stratégiques.

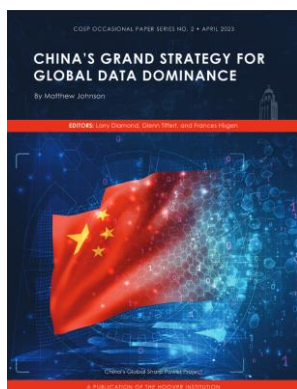
[explosionsartigen Zunahme von KI-Anwendungen](#) die den Umgang mit Daten täglich komplizierter machen, könnten Unternehmen und Institutionen einige Werkzeuge gut gebrauchen.

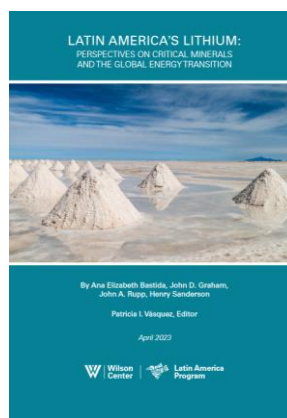
- **Europa in Kürze** - ▶ Die [souveräne Cloud](#) könnte zur *Arlésienne 4.0* werden. ▶ Der Data Act stösst auf [Gegenwind](#), da Unternehmen um ihre Wettbewerbsfähigkeit fürchten. ▶ Wir werden ein neues Akronym lernen müssen: [ECCC](#) für das *European Cybersecurity Competence Centre and Network*, das gerade in Bukarest eröffnet wurde. Es bleibt zu hoffen, dass die Aktivitäten dieses Zentrums sich von den nationalen Stellen, der [ENISA](#), dem [CCDCOE](#) oder dem [Hybrid CoE](#) unterscheiden und einen echten Mehrwert bieten werden. ▶ Zuletzt sollten wir [das Manifest der JEDI](#) - *Joint European Disruptive Initiative* zur Kenntnis nehmen, die die europäischen Staaten um eine [DARPA](#)-ähnliche Initiative versammeln will, um den Kontinent wieder in die Reihe der technologischen Mächte zurückzuführen, insbesondere durch eine agile Regierungsführung, weg von den ineffizienten europäischen Standards und um eine begrenzte Anzahl von strategischen Themen herum.

BOOKS & REPORTS

Voici les livres et publications d'intérêts découverts durant nos recherches des dernières trois semaines.

Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in den letzten drei Wochen gefunden haben.





En bref - ▶ Pour **TikTok**, la discussion a porté jusqu'ici sur la confidentialité des données et la manipulation individuelle des contenus, mais le problème clé se trouve au niveau de [l'algorithme de recommandation](#) qui permet à la Chine d'établir un profil de masse des utilisateurs et de conduire des opérations d'influence à grande échelle. ▶ Avec le COVID, la Suisse s'est retrouvée avec 9 millions d'experts en virologie et avec **ChatGPT** nous sommes tous devenus des experts en IA. Pour mériter ce titre, prenons le temps de nous documenter sur son identité ([1](#), [2](#), [3](#)). ▶ Et qui se souvient de la cyberattaque contre **SolarWinds**, à ce jour la plus grande attaque connue contre la chaîne d'approvisionnement cyber? Un [rapport détaillé](#) expose désormais le mode opératoire des Russes.

Et notre fascination pour l'immensité de l'espace ne faiblit pas. On vous invite à admirer la première ceinture d'astéroïdes jamais découverte en dehors du système solaire par le [James Webb Space Telescope](#) (JWST).

Nous vous souhaitons une enrichissante découverte des [articles et liens](#) sélectionnés et nous réjouissons de vous retrouver bientôt.

In Kürze - ▶ Bei **TikTok** drehte sich die Diskussion bisher um den Datenschutz und die individuelle Manipulation von Inhalten, aber das Schlüsselproblem liegt im [Empfehlungsalgorithmus](#), der es China ermöglicht, ein Massenprofil der Nutzer zu erstellen und gross angelegte Beeinflussungsoperationen durchzuführen. ▶ Mit COVID hatte die Schweiz 9 Millionen Virologieexperten und mit **ChatGPT** sind wir alle zu KI-Experten geworden. Um diesen Titel zu verdienen, sollten wir uns die Zeit nehmen, uns über seine Identität zu informieren ([1](#), [2](#), [3](#)). ▶ Und wer erinnert sich vom Cyberangriff auf **SolarWinds**, der bis heute der grösste bekannte CyberSupplyChain-Angriff ist? Es gibt nun einen [detaillierten Bericht](#), der die Vorgehensweise der Russen aufzeigt.

Und unsere Faszination für die Weite des Welt-raums ist ungebrochen. Wir laden sie ein, den ersten Asteroidengürtel zu bewundern, den das [James Webb Space Telescope](#) (JWST) ausserhalb unseres Sonnensystems entdeckt hat.

Wir wünschen Ihnen viel Spass beim Entdecken der ausgewählten [Artikel und Links](#) und freuen uns darauf, Sie bald wiederzusehen.





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.