

Les billetsⁱ 2021 de **digiVolution** / **digiVolution's 2021 Newsletters**
[22.11.2021 – semaines 45-46]


" Space Junk "

Chers Lectrices et Lecteurs,

Nous avons le plaisir de vous adresser les **dV-News 45 & 46** de **digiVolution** et notre sélection d'[articles et de liens](#). Et si vous avez manqué une précédente édition, nos newsletters vous attendent sagement [en ligne](#).

Dans l'actualité de la quinzaine écoulée, c'est à nouveau vers l'espace que notre attention a été attirée, cette fois en raison des déchets spatiaux, ou **space junk**, provoqués par la Russie. Cette action irresponsable, qui a aussi mis en danger l'ISS et ses occupants, a démontré une fois encore l'absence de règles dans l'espace et les conséquences possibles de tels actes sur une infrastructure spatiale désormais vitale au quotidien.

Il ne s'agit certes pas du même sujet, mais les trois exemples qui suivent, pris dans l'actualité de la quinzaine écoulée, souffrent du même mécanisme de *laisser-faire généralisé*.


 **Les objets connectés** – Depuis les années 2007-2008, les études se sont multipliées qui mettent en évidence les défaillances de [sécurité des objets connectés](#) et leurs conséquences. Nombreux sont les acteurs économiques qui persistent pourtant à y voir d'abord – comme dans l'espace – les [profits](#) potentiels. Pourtant, comme avec les déchets de l'espace, on continue à multiplier par milliards des objets non sécurisés qui fragilisent tout le cyberspace. Et si notre nouveau [Centre national de test](#) est une excellente initiative, elle reste modeste face à l'immensité de ce problème non résolu.

Liebe Leserinnen und Leser,

Wir freuen uns, Ihnen die **dV-News 45 & 46** von **digiVolution** und unsere [Auswahl an Artikeln und Links](#) zukommen zu lassen. Und falls Sie eine der vorherigen Ausgaben unseres Newsletters verpasst haben, warten diese [online](#) auf Sie.


In den Nachrichten der letzten zwei Wochen wurde unsere Aufmerksamkeit erneut auf den Weltraum gelenkt, diesmal wegen des von Russland verursachten Weltraummülls oder **Space Junk**. Diese unverantwortliche Aktion, die auch die ISS und ihre Insassen in Gefahr brachte, machte wieder einmal deutlich, dass es im Weltraum keine Regeln gibt und welche Auswirkungen solche Handlungen auf eine Weltrauminfrastruktur haben können, die für unser tägliches Leben von vitaler Bedeutung ist.

Es handelt sich zwar nicht um dasselbe Thema, aber die folgenden drei Beispiele aus den Nachrichten der letzten zwei Wochen unterliegen demselben Mechanismus des *allgemeinen Laissez-faire*.

 **Vernetzte Objekte** – Seit den Jahren 2007-2008 gibt es immer mehr Studien, die auf [Sicherheitsmängel bei vernetzten Objekten](#) und deren Folgen hinweisen. Viele Wirtschaftsakteure beharren jedoch darauf, in erster Linie – wie im Weltraum – die potenziellen [Gewinne](#) zu sehen. Doch wie bei den Abfällen aus dem Weltraum werden weiterhin Milliarden von unsicheren Objekten produziert, die den gesamten Cyberraum schwächen. Unser neues [Nationales Testzentrum](#) ist zwar eine ausgezeichnete Initiative, aber angesichts des




 **La Chine et Taïwan** – Les signaux négatifs s'accumulent autour de la Chine. Souvenons-nous du [Document nr. 9](#) du Parti communiste chinois en 2013 qui montre son rejet des valeurs qui ont régit le monde depuis la fin de la Seconde Guerre mondiale. Désormais il ne se passe pas non plus une semaine sans qu'il soit question *d'éviter* un conflit armé qui semble devenu inéluctable entre les USA et la Chine, notamment autour de [Taïwan](#). Personne ne pourra dire *nous n'avons pas vu venir*. Pourtant qu'est-ce qui est concrètement fait pour éviter la catastrophe annoncée en particulier d'une interruption de l'approvisionnement en semi-conducteurs produits à Taïwan?

 **Les médias sociaux** – Les témoignages se succèdent quant à la nocivité de certains médias sociaux. De géniales inventions, mais comme pour toute voiture surpuissante, à ne pas mettre entre toutes les mains! Alors quand on constate qu'il n'est pas possible d'éviter les débordements et abus alors il faut encadrer. Est-ce encore possible? Réjouissons-nous dans l'intervalle que la [Confédération](#) s'empare du sujet et l'[étude](#) enfin. Mais comme le montrait déjà Chapatte en 2004, les contenus nauséabonds ne sont rien de nouveau. Et qu'a-t-on fait durant ces derniers 17 ans?

immenses Ausmasses dieses ungelösten Problems ist ihre Wirkung bescheiden.

 **China und Taiwan** – Um China häufen sich die negativen Signale. Wir erinnern uns an das [Dokument Nr. 9](#) der Kommunistischen Partei Chinas aus dem Jahr 2013, das ihre Ablehnung der Werte zeigt, die die Welt seit dem Ende des Zweiten Weltkriegs dominiert haben. Es vergeht kaum eine Woche, in der nicht über die Vermeidung eines bewaffneten Konflikts zwischen den USA und China gesprochen wird, der scheinbar unausweichlich geworden ist, insbesondere um [Taiwan](#). Niemand kann sagen, *wir haben es nicht kommen sehen*. Doch was wird konkret getan, um die angekündigte Katastrophe u.a. einer Unterbrechung der Versorgung mit in Taiwan produzierten Halbleitern zu verhindern?

 **Soziale Medien** – Es gibt immer wieder Berichte über die Schädlichkeit bestimmter sozialer Medien. Geniale Erfindungen, aber wie bei jedem übermächtigen Gerät, sollte man sie nicht in alle Hände geben. Wenn man also feststellt, dass es nicht möglich ist, Ausschweifungen und Missbrauch zu verhindern, muss man den Rahmen festlegen. Ist das noch möglich? Inzwischen freuen wir uns, dass der [Bund](#) das Thema [aufgreift](#) und es endlich untersucht. Aber wie Chapatte bereits 2004 aufzeigte, sind üble Inhalte nichts Neues. Und was wurde in den letzten 17 Jahren getan?



Chapatte, Bilan, 01.02.2004

Pour terminer ce billet sur une note optimiste, réjouissons-nous de deux nouvelles.

- 🚩 Après un premier essai au DDPS malheureusement vite oublié au fond d'un tiroir de l'administration fédérale en 2015, la Suisse dispose à nouveau d'une [liste des institutions publiques de formation en cybersécurité](#). Merci au NCSC. Il ne reste plus qu'aux responsables en charge des infrastructures digitales à prendre rendez-vous et d'aller se mettre à jour! Car l'actualité le montre, les cyberattaques ce n'est pas que pour les autres. Plus [d'un tiers des PME](#) en a été victimes durant l'année écoulée.
- 🚩 Après des années de tergiversation, le projet SCION de l'ETHZ semble lentement s'imposer. Mais comment est-il possible qu'il faille aussi longtemps pour implémenter une solution aussi efficace et dont les coûts de déploiement restent par ailleurs modiques? Ne

Um diesen Beitrag mit einer optimistischen Note zu beenden, freuen wir uns über zwei Neuigkeiten.

- 🚩 Nach einem ersten Versuch im VBS, der 2015 leider schnell in einer Schublade der Bundesverwaltung vergessen wurde, verfügt die Schweiz nun wieder über eine [Liste der öffentlichen Institutionen, die Schulungen im Bereich Cybersicherheit](#) anbieten. Vielen Dank an das NCSC. Jetzt müssen die Verantwortlichen für die digitale Infrastruktur nur noch einen Termin vereinbaren und sich auf den neuesten Stand bringen lassen! Denn wie die Nachrichten zeigen, sind Cyberangriffe nicht nur für die anderen da. Mehr als ein [Drittel der KMUs](#) war im vergangenen Jahr Opfer von Cyberangriffen.
- 🚩 Nach jahrelangem Hin und Her scheint sich das SCION-Projekt der ETHZ langsam durchzusetzen. Aber wie ist es möglich, dass es so



serait-ce que pour nos infrastructures critiques. Car oui s'il est juste que le conseil fédéral ait retoqué la motion [Gapany](#) (de même qu'il faut tordre le cou à cette idée de [secrétariat d'État](#) qui revient sur la scène tous les 5 ans), comment justifier que SCION n'ait pas été imposé jusqu'ici aux opérateurs d'infrastructures vitales pour sécuriser leurs opérations?

Nous vous souhaitons une enrichissante lecture et nous réjouissons de vous retrouver dans 15 jours pour notre prochain billet dont le sujet principal sera le premier anniversaire de *dig*iVolution.

lange dauert, eine so effiziente Lösung zu implementieren, die zudem nur geringe Kosten verursacht? Und sei es nur für unsere kritischen Infrastrukturen. Denn auch wenn es richtig ist, dass der Bundesrat die Motion [Gapany](#) abgelehnt hat (ebenso wie die Idee eines [Staatssekretariats](#), das alle fünf Jahre wieder auf den Plan tritt), wie lässt es sich rechtfertigen, dass SCION den Betreibern kritischer Infrastrukturen bislang nicht vorgeschrieben wurde, um ihre Operationen zu sichern?

Wir wünschen Ihnen eine interessante Lektüre und freuen uns darauf, Sie in zwei Wochen für unseren nächsten Beitrag wiederzusehen, dessen Hauptthema der erste Geburtstag von *dig*iVolution sein wird.

ⁱ Depuis le 8 janvier 2021, *dig*iVolution 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. Ces articles sont disponibles à l'adresse <https://www.digivolution.swiss/news/>. Les personnes intéressées trouveront sur cette même page le lien pour s'y inscrire. /// Seit dem 8. Januar 2021 veröffentlicht *dig*iVolution regelmässig einen Newsletter, der von einer Auswahl «handverlesener» Artikel begleitet wird, die die Komplexität der mit der digitalen Mutation verbundenen Herausforderungen veranschaulichen. Diese Artikel finden Sie unter <https://www.digivolution.swiss/news/>. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.