digiVolution
Prepare for the next

*d*VNews

Les billets de *digi*Volution / *digi*Volution's Newsletters
[15.10.2024 – Édition / Ausgabe Nr. 105]

Cyber kills

Chers Lectrices et Lecteurs,

Nous avons le plaisir de vous adresser la 105ème *d*VNews (14-2024) et sa sélection d'articles et liens. Tous nos regrets pour n'avoir pas pu vous revenir plus vite, mais comme vous le découvrirez, cette édition compense par sa richesse.

En 2010, le monde découvrait que l'Iran était la cible d'une opération baptisée ensuite OLYMPIC GAMES et que divers auteurs attribuent aux services israéliens et américains. STUXNET, un ver qualifié alors de *première cyberarme*, en fut l'instrument. Les preuves publiques formelles manquent encore, mais les articles sur le sujet admettent que l'objectif de l'opération était de saboter les centrifugeuses servant à l'enrichissement de l'uranium pour retarder le programme d'armement nucléaire iranien. STUXNET venait ainsi d'illustrer les liens directs entre le monde physique et le monde virtuel.

Liebe Leserinnen und Leser,

Wir freuen uns, Ihnen unsere 105. *d*VNews (14-2024) mit einer Auswahl an Artikeln und Links zukommen zu lassen. Wir bedauern, dass wir uns nicht schneller bei Ihnen melden konnten, dafür gleicht diese Ausgabe durch ihren Umfang.

Im Jahr 2010 erfuhr die Welt, dass Iran das Ziel einer Operation war, die später OLYMPIC GAMES genannt wurde und die von verschiedenen Autoren den israelischen und amerikanischen Diensten zugeschrieben wurde. STUXNET, ein Wurm, der damals als *erste Cyberwaffe* bezeichnet wurde, war das Instrument. Formale öffentliche Beweise fehlen noch, aber in den Artikeln zu diesem Thema wird eingeräumt, dass das Ziel der Operation war, die Zentrifugen für die Urananreicherung zu sabotieren, um das iranische Atomwaffenprogramm zu

Dear readers,

We are pleased to send you our 105th *d*VNews (14-2024) with a selection of articles and links. We're sorry we couldn't get back to you sooner, but as you'll discover, this edition makes up for it in richness.

In 2010, the world discovered that Iran was the target of an operation later dubbed OLYMPIC GAMES, which various authors attribute to Israeli and American services. STUXNET, a worm described at the time as the *world's first cyberweapon*, was the tool. Formal public proof is still lacking, but articles on the subject admit that the aim of the operation was to sabotage the centrifuges used for uranium enrichment in order to delay Iran's nuclear weapons program. STUXNET thus illustrated the direct links between the physical and virtual worlds.

The attacks on Hezbollah using *pagers* and *walkie-talkies* on September 17 and 18 2024 follow a similar

Les attaques contre le Hezbollah au moyen des *pagers* et des *talkie walkies* les 17 et 18 septembre 2024 s'inscrivent dans une logique similaire. Comme en 2010, Israël laisse également planer le doute quant aux auteurs et à leurs méthodes.

De fait il s'agit là d'une opération d'information dont le but est de briser le commandement de l'ennemi. Cette ligne d'opération offre un avantage clé : le temps. Elle peut en effet commencer en période de paix, par exemple en matière de dissuasion et d'influence, rester sous le seuil de la guerre, par exemple avec des cyberattaques dont l'intensité ne justifie pas une réaction militaire, puis se prolonger durant la guerre.

Nombreux sont les pays qui ont compris l'importance de la dimension informationnelle (au sens large) et disposent d'une **doctrine pour les opérations d'information**. De manière très résumée, cette doctrine repose sur trois piliers : **des effets dans le cyberespace, dans la sphère informationnelle** (guerre d'influence / guerre cognitive) **et dans la sphère électromagnétique**. Plus rares sont les pays qui possèdent de vrais moyens dans ces trois dimensions et de la capacité à les synchroniser avec les autres lignes d'opération, air, terre, mer, espace.

Il ne nous appartient pas de qualifier les opérations israéliennes contre le Hamas

verzögern. STUXNET war ein Beispiel für die direkte Verbindung zwischen der physischen und der virtuellen Welt.

Die Angriffe auf die Hisbollah mit Hilfe von *Pagern* und *Walkie-Talkies* am 17. und 18. September 2024 folgen einer ähnlichen Logik. Wie im Jahr 2010 lässt Israel auch hier Zweifel an den Urhebern und ihren Methoden aufkommen.

Tatsächlich handelt es sich hier um eine Informationsoperation, die darauf abzielt, die Führung des Feindes zu zerschlagen. Diese Operationslinie hat einen entscheidenden Vorteil: Zeit. Sie kann in Friedenszeiten beginnen, z.B. im Bereich der Abschreckung und Einflussnahme, unterhalb der Kriegsschwelle bleiben, z.B. mit Cyberangriffen, deren Intensität keine militärische Reaktion rechtfertigen, um dann während des Krieges fortgesetzt zu werden.

Viele Länder haben die Bedeutung der Informationsdimension (im weitesten Sinne) erkannt und verfügen über eine **Doktrin für Informationsoperationen**. Diese Doktrin beruht auf drei Säulen: **Auswirkungen im Cyberraum, in der Informationssphäre** (Einflusskrieg / kognitive Kriegsführung) **und in der elektromagnetischen Sphäre**. Nur wenige Länder verfügen jedoch über echte Mittel in diesen drei Dimensionen und

pattern.
As in 2010, Israel is also casting doubt on the perpetrators and their methods.

In fact, this is an information operation whose aim is to break the enemy's command. This line of operation offers a key advantage: time. It can begin in times of peace, for example in terms of deterrence and influence, remain below the threshold of war, for example with cyber-attacks whose intensity does not justify a military response, and then continue during war.

Many countries have understood the importance of the information dimension (in the broadest sense) and have developed a **doctrine for information operations**. In a nutshell, this doctrine is based on three pillars: **effects in cyberspace, in the informational sphere** (influence warfare / cognitive warfare) **and in the electromagnetic sphere**. Only few countries have real resources in these three dimensions, and the ability to synchronize them with other lines of operation: air, land, sea and space.

It is not up to us to qualify Israels operations against Hamas and Hezbollah from the comfort of our country, which has lived in peace for 177 years and whose last Sonderbund war lasted 23 days, killing 93 people and wounding 510. However, it must be said that in the

et le Hezbollah depuis le confort de notre pays qui vit en paix depuis 177 ans et dont la dernière guerre du Sonderbund a duré 23 jours et aurait fait 93 morts et 510 blessés. Force est cependant de constater que dans le conflit qui déchire le Proche-Orient, les opérations israéliennes « cochent » toutes les cases des opérations d'information.

OUI, le cyberespace tue !

über die Fähigkeit, diese mit den anderen Operationslinien Luft, Land, See und Weltraum zu synchronisieren.

Es steht uns nicht zu, die israelischen Operationen gegen die Hamas und die Hisbollah aus der Komfortzone unseres Landes heraus zu bewerten, das seit 177 Jahren in Frieden lebt und dessen letzter Sonderbundskrieg 23 Tage dauerte und 93 Tote sowie 510 Verletzte gefordert haben soll. Es bleibt jedoch festzustellen, dass im Nahostkonflikt die israelischen Operationen alle Kästchen der Informationsoperationen «ankreuzen».

JA, der Cyberraum tötet!

conflict that is tearing the Middle East apart, Israeli operations are « ticking » all the information operations boxes.

YES, cyberspace kills!

Ne nous laissons pas gagner par la tentation des spéculations et concentrons-nous sur notre niveau. Comme avec STUXNET, les attaques contre le Hezbollah ont emprunté les chemins complexes, souvent non considérés et/ou non maîtrisés des **chaînes**

Lassen wir uns nicht von den Spekulationen verleiten und konzentrieren wir uns auf unsere Ebene. Wie bei STUXNET haben die Angriffe auf die Hisbollah die komplexen, oftmals nicht beachteten und/oder nicht beherrschten Wege der **Lieferketten** genutzt. Was

Let's not get carried away by the temptation to speculate and concentrate on our level. As with STUXNET, the attacks on Hezbollah have taken the complex, often unconsidered and/or unmastered paths of **supply chains**. What are the consequences? What possibilities do these

d'approvisionnement. Quelles en sont les conséquences ? Quelles possibilités ces opérations ouvrent-elles et suggèrent-elles à l'ensemble des acteurs de la menace en recherche permanente d'idées alors que nos défenseurs peinent déjà à suivre ? Les IoT / OT représentent-ils un vecteur d'attaque possible? Si oui, qui doit s'en prémunir et comment ? Nous entendons trop de dénégations et d'avis isolés fondés sur aucune analyse sérieuse des risques. Ces événements vont-ils, comme l'affaire CrowdStrike du 19 juillet 2024 et les millions d'écrans bleus, disparaître dans l'oubli ? D'ailleurs, qui se souvient des BSoD ? Qui en a tiré des leçons et pris des mesures concrètes ? En Suisse, sommes-nous *équipés* pour nous défendre dans la sphère informationnelle ? Nos moyens en matière de cybersécurité et de cyberdéfense sont-ils à la hauteur des enjeux ? Nous parlons ici du pays dans son ensemble dont personne ne semble connaître le réel degré de maturité face à ces phénomènes.

Voici encore un domaine où une cartographie digne de ce nom serait essentielle pour savoir où notre pays doit vraiment investir dans sa défense.

sind die Folgen davon? Welche Möglichkeiten eröffnen und suggerieren diese Operationen für alle Bedrohungsakteure, die ständig nach neuen Ideen suchen, während unsere Verteidiger bereits Mühe haben, Schritt zu halten? Sind IoT / OT ein möglicher Angriffsvektor? Wenn ja, wer muss sich dagegen schützen und wie? Wir hören zu viele Dementis und Einzelmeinungen, die auf keiner ernsthaften Risikoanalyse basieren. Werden diese Ereignisse, wie die CrowdStrike-Affäre vom 19. Juli 2024 und die Millionen blauer Bildschirme, in Vergessenheit geraten? Wer erinnert sich überhaupt noch an die BSoD? Wer hat daraus gelernt und konkrete Massnahmen ergriffen? Sind wir in der Schweiz *ausgerüstet*, um uns in der Informationssphäre zu verteidigen? Sind unsere Mittel für Cybersicherheit und Cyberdefense den Herausforderungen gewachsen? Wir sprechen hier über das Land als Ganzes, von dem niemand zu wissen scheint, wie reif es in Bezug auf diese Phänomene wirklich ist.

Dies ist ein weiterer Bereich, in dem eine gute Kartographie wichtig wäre, um zu wissen, wo unser Land wirklich in seine Verteidigung investieren sollte.

operations open up and suggest to all threat actors in constant search of ideas, while our defenders are already struggling to keep up? Do IoT/OT represent a possible attack vector? If so, who needs to protect themselves and how? We hear too many denials and isolated opinions based on no serious risk analysis. Will these events, like the CrowdStrike affair of July 19 2024 and the million blue screens, disappear into oblivion? Besides, who remembers the BSoDs? Who has learned from them and taken concrete action? In Switzerland, are we *equipped* to defend ourselves in the information sphere? Are our cybersecurity and cyberdefense resources up to the challenge? We are talking here about the country as a whole, about which no one seems to know how mature it really is in relation to these phenomena.

Here's another area where proper mapping would be essential to know where our country really needs to invest in its defense.

BOOKS & REPORTS

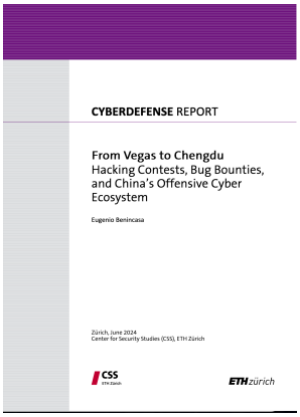
Ci-après nous, vous présentons la liste des publications d'intérêt découvertes lors de nos recherches. Un résumé et leurs coordonnées sont disponibles sur dVPedia.

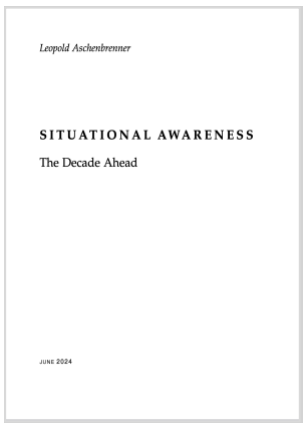
BOOKS & REPORTS

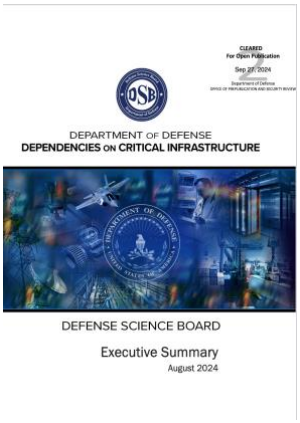
Untenstehend ist eine Liste der verfügbaren Publikationen von Interesse, die wir bei unseren Recherchen entdeckt haben. Eine Zusammenfassung und Kontaktinformationen finden Sie auf dVPedia.

BOOKS & REPORTS

The following is a list of publications of interest discovered during our research. A summary and contact details are available on dVPedia.







ACTUALITES

▶ **La désinformation sous un angle historique** – Les guerres de religion qui ont ravagé l'Europe dans le sillage de la révolution de l'imprimerie suggèrent que la révolution numérique pourrait alimenter la violence à une échelle similaire dans les années et les décennies à venir. La vitesse et l'échelle inédites de la diffusion et de la manipulation de l'information peuvent cependant provoquer des désordres globaux beaucoup plus rapidement que par le passé. L'attaque du Capitole en janvier 2021, attisée par de fausses histoires dans les médias sociaux au sujet des élections américaines de 2020, ou encore les récentes émeutes en Grande-Bretagne n'en sont que les signes précurseurs. Il ne se passe pas une semaine sans un nouveau rapport alarmiste et des exemples en matière de manipulation et d'influence. La guerre cognitive a largement débuté et la myopie historique de l'industrie technologique pourrait s'avérer être son plus grand crime. C'est en tout cas

AKTUELLES

▶ **Desinformation aus historischer Sicht** – Die Religionskriege, die Europa im Nachgang der Revolution des Buchdrucks verwüsteten, legen nahe, dass die digitale Revolution in den kommenden Jahren und Jahrzehnten Gewalt in ähnlichem Ausmass schüren könnte. Die beispiellose Geschwindigkeit und das Ausmass der Verbreitung und Manipulation von Informationen können jedoch viel schneller als in der Vergangenheit zu globalen Unruhen führen. Der Angriff auf das Kapitol im Januar 2021, der durch Fake News in den sozialen Medien über die US-Wahlen 2020 angeheizt wurde, und die jüngsten Unruhen in Grossbritannien sind nur die Vorboten davon. Es vergeht keine Woche ohne neue Schreckensmeldungen und Beispiele für Manipulation und Einflussnahme. Der kognitive Krieg hat bereits begonnen und die historische Kurzsichtigkeit der Technologieindustrie könnte

NEWS

▶ **Disinformation in historical perspective** - The religious wars that ravaged Europe in the wake of the printing revolution suggest that the digital revolution could fuel violence on a similar scale in the years and decades to come. The unprecedented speed and scale of information dissemination and manipulation could provoke global disorder much more rapidly than in the past. The attack on the Capitol in January 2021, fanned by fake news in social media about the illegality of the 2020 US elections, or the recent riots in Great Britain were just the beginning. Not a week goes by without a new alarmist report and examples of manipulation and influence. The cognitive war is well underway, and the technology industry's historical short-sightedness could prove to be its greatest crime. At any rate, that's the thought behind an article that has the merit of posing the question, while also recalling a famous phrase by Abraham Lincoln: «You can

la réflexion que suggère un article qui a le mérite de poser la question tout en rappelant aussi une célèbre phrase d'Abraham Lincoln : « *Vous pouvez tromper une partie du peuple tout le temps, et tout le peuple une partie du temps, mais vous ne pouvez pas tromper tout le peuple tout le temps* ».

▶ **Subsidiarité** – En matière de lutte contre les cyberincidents, le Conseil fédéral souhaite un appui subsidiaire facilité des moyens de l'armée au profit de l'Office fédéral de la cybersécurité OFCS. Est-ce une bonne chose ? Sans aucun doute, à la condition que cela ne soit pas une excuse pour ne pas donner à l'OFCS les moyens dont il a un urgent besoin. Il s'agit aussi de rester réaliste quant aux tâches qui peuvent être réellement confiées aux spécialistes de l'armée. Ce qui interpelle, c'est le délai de 2026 pour proposer une solution. Faudra-t-il encore 2 ans pour la concrétiser ? À part cette contradiction, nous encourageons vivement la lecture de ce document que l'on peut qualifier d'unique pour deux raisons. Tout d'abord il représente un **travail important et très bienvenu d'explication de ce qu'est la subsidiarité**. Ensuite, il est une **lecture impérative pour comprendre de quelles instances dispose la Confédération en matière de cybersécurité**.

sich als ihr grösstes Verbrechen erweisen. Dies ist jedenfalls die Überlegung, die ein Artikel aufwirft und gleichzeitig das Verdienst hat, im Gegenzug an einen berühmten Satz von Abraham Lincoln zu erinnern: «*Sie können einen Teil des Volkes die ganze Zeit täuschen und das ganze Volk einen Teil der Zeit, aber Sie können nicht das ganze Volk die ganze Zeit täuschen*».

▶ **Subsidiarität** - Im Bereich der Bekämpfung von Cybervorfällen wünscht der Bundesrat eine erleichterte subsidiäre Unterstützung des Bundesamtes für Cybersicherheit BACS durch Mittel der Armee. Ist dies eine gute Sache? Zweifellos, aber unter der Bedingung, dass dies keine Entschuldigung dafür ist, dem BACS nicht die dringend benötigten Mittel zur Verfügung zu stellen. Es geht auch darum, realistisch zu bleiben, was die Aufgaben betrifft, die den Spezialisten der Armee tatsächlich anvertraut werden können. Was auffällt, ist die Frist bis 2026, um eine Lösung vorzuschlagen. Wird es noch zwei Jahre dauern, bis sie umgesetzt wird? Abgesehen von diesem Widerspruch, empfehlen wir dringend die Lektüre dieses Dokuments, das aus zwei Gründen als einzigartig bezeichnet werden kann. Erstens stellt es eine **wichtige und sehr willkommene Arbeit** dar,

fool some of the people all of the time, and all of the people some of the time, but you cannot fool all of the people all of the time».

▶ **Subsidiarity** - When it comes to combating cyber incidents, the Federal Council wants to facilitate the subsidiary support of military resources for the National Cyber Security Center NCSC. Is this a good thing? Undoubtedly, provided this is not an excuse not to give the NCSC the resources it urgently needs. It's also a question of remaining realistic about the tasks that can really be entrusted to army specialists. The deadline of 2026 for proposing a solution is particularly worrying. Will it take another 2 years to put it into practice? Apart from this contradiction, we strongly encourage you to read this document, which can be described as unique for two reasons. Firstly, it represents an **important and very welcome effort to explain what subsidiarity is** all about. Secondly, it is **essential reading if we are to understand which authorities the Confederation has at its disposal in the field of cybersecurity**.

In this respect, it is interesting to revisit the speech given by the President of the Confederation at the National Conference on Cybersecurity on September 26 in Berne. Clearly, the importance of cybersecurity is

Dans ce sens il est intéressant de revenir sur le discours de la Présidente de la Confédération lors de la Conférence nationale sur la cybersécurité le 26 septembre dernier à Berne. À l'évidence, l'importance de la cybersécurité est comprise dans les plus hautes sphères. Nos incessantes observations et questions montrent cependant l'espace d'amélioration considérable qui subsiste entre les discours et les actes concrets…

um **zu erklären, was Subsidiarität ist**. Zweitens ist es eine **Pflichtlektüre, um zu verstehen, über welche Instanzen der Bund im Bereich der Cybersicherheit verfügt**.

In diesem Sinne ist es interessant, auf die Rede der Bundespräsidentin anlässlich der nationalen Cybersicherheitskonferenz a m 26. September 2024 in Bern zurückzukommen. Es ist offensichtlich, dass die Bedeutung der Cybersicherheit in den höchsten Sphären verstanden wird. Unsere ständigen Beobachtun-gen und Fragen zeigen jedoch, dass zwischen den Reden und den konkreten Handlungen noch viel Raum für Verbesserungen besteht…

understood at the highest levels. However, our constant observations and questions show that there is still considerable room for improvement between words and deeds…

▶ JO de Paris – *d*VCyberGroup, société opérationnelle de la fondation *digi*Volution a eu la chance d'être mandatée pour contribuer à cette immense manifestation qui a déjoué quasiment tous les pronostics

▶ *Olympia in Paris* – *d*VCyberGroup, das operative Unternehmen der Stiftung *digi*Volution, erhielt den Auftrag, zu dieser riesigen Veranstaltung beizutragen, die fast alle kataklysmischen Prognosen wiederlegte.

⌥ Olympic Games in Paris - *d*VCyberGroup, the operating company of the *digi*Volution foundation, was commissioned to contribute to this huge event, which defied almost all cataclysmic forecasts. Some

cataclysmiques. Certains estimeront peut-être que les rapports officiels ont embelli la situation ? Notre expérience confirme cependant le bilan sécuritaire positif des Jeux. Ce résultat est explicable.

Les précautions d'usage ont été prises. Gestion des risques, mesures de sécurité prises et contrôlées, gestion de crise en place et entraînée, monitoring et appréciation permanents de la situation (en clair : renseignement à 360°). Il n'en fallait pas plus pour que les cyberassaillants se cassent les dents sur un noyau trop solide et qu'ils reportent leurs attaques sur des cibles plus accessibles, c'est-à-dire la chaîne d'approvisionnement. Mais ces actions, par ailleurs non rentables pour les agresseurs, ont eu un faible impact et n'ont pas porté un préjudice significatif aux Jeux. Seules les statistiques nationales pourront cependant dire si les criminels ont profité que les services de l'État soient absorbés par les JO pour pousser leurs pions ailleurs.

Les assaillants avec des objectifs politiques étaient occupés ailleurs. Les acteurs de la menace russes certainement fâchés par l'exclusion de leur pays des JO sont en effet aux prises avec une guerre dont les enjeux sont tout autre. Avec la guerre au Moyen-Orient, les acteurs de la menace qui auraient pu profiter de l'événement pour répéter le *coup de Munich* de 1972 avaient aussi d'autres priorités.

Einige werden vielleicht der Meinung sein, dass die offiziellen Berichte die Situation verschönert haben? Unsere Erfahrung bestätigt jedoch die positive Sicherheitsbilanz der Spiele. Dieses Ergebnis ist erklärbar.

Die üblichen Vorsichtsmassnahmen wurden getroffen. Risikomanagement, Sicherheitsmassnahmen wurden ergriffen und kontrolliert, Krisenmanagement wurde eingerichtet und trainiert, die Lage wurde ständig überwacht und beurteilt (im Klartext: 360°-Nachrichtendienst). Es hätte nicht viel gefehlt, dass sich die Cyberangreifer an einem zu starken Grundgerüst die Zähne ausbeissen und ihre Angriffe auf leichter zugängliche Ziele, d.h. die Lieferkette, verlagern. Aber diese Aktionen, die für die Angreifer nicht profitabel waren, hatten nur eine geringe Wirkung und fügten den Spielen keinen bedeutenden Schaden zu. Nur die nationalen Statistiken können jedoch zeigen, ob die Kriminellen die Tatsache, dass die staatlichen Dienste von den Olympischen Spielen absorbiert wurden, dazu nutzten, um anderswo ihre Ziele zu verfolgen.

Angreifer mit politischen Zielen waren anderweitig beschäftigt. Die Akteure der russischen Bedrohung, die sicherlich über den Ausschluss ihres Landes von den Olympischen Spielen

may feel that the official reports embellished the situation? However, our experience confirms the positive safety record of the Games. This result can be explained.

The usual precautions were taken. Risk management, security measures taken and controlled, crisis management in place and trained, constant monitoring and assessment of the situation (in short: 360° intelligence). This was all it took for cyber-assailants to break their teeth on a too solid core and shift their attacks to more accessible targets, i.e. the supply chain. But these actions, which were not profitable for the attackers, had little impact and did not cause significant damage to the Games. However, only national statistics will be able to tell whether criminals took advantage of the fact that government services were absorbed by the Olympics to push their pawns elsewhere.

Attackers with political objectives were busy elsewhere. The Russian threat actors, undoubtedly angered by their country's exclusion from the Olympics, are in fact grappling with a war whose stakes are quite different. With the war in the Middle East, the threat actors who could have used the event to repeat the *Munich coup of* 1972 also had other priorities.

A mixture of skill, action and opportunism ensured that the great sporting event went off without a hitch. However, it would be wrong to deduce an

Un mélange de compétences, de mesures réellement prises et d'opportunisme a donc permis à la grande fête du sport de bien se dérouler. Il serait cependant erroné d'en déduire une règle absolue, car les prochains jeux en Italie en 2026, aux USA en 2028 et en France en 2030 auront tous des conditions différentes. Paris a montré la voie à prendre en matière de cybersécurité et il faut espérer que la Suisse sera à la hauteur pour l'Eurovision en mai 2025. Car ne nous méprenons pas, l'European Song Contest est aussi une manifestation géante qui sera aussi dans le collimateur de différents acteurs malveillants.

À l'avenir il s'agira cependant aussi de cesser d'annoncer des chiffres fantastiques de milliards d'attaques. Car un ping n'est pas une cyberattaque. Et quand un voleur observe la page web d'une banque, ce n'est pas encore un braquage…

▶ **Telegram** – Comment interpréter l'arrestation de Pavel Durov et les charges qui pèsent sur lui. Coup d'arrêt bienvenu aux comportements de cowboy de certains patrons de société de la tech qui donnent aux criminels des armes qu'ils ne devraient pas avoir tout en ne collaborant pas (assez) avec les autorités légitimes des États ? Mais si on arrête Durov, que fait-on alors des Musk, Pichai et Zuckerberg dont les sociétés ne cessent d'être accusées et condamnées pour ne pas respecter les règles ? Cette

verärgert sind, kämpfen in der Tat mit einem Krieg, bei dem es um etwas ganz anderes geht. Angesichts des Krieges im Nahen Osten hatten die Bedrohungsakteure, die die Veranstaltung hätten nutzen können, um den *Münchner Coup* von 1972 zu wiederholen, auch andere Prioritäten.

Eine Mischung aus Kompetenz, tatsächlich ergriffenen Massnahmen und Opportunismus sorgte für einen reibungslosen Ablauf des grossen Sportfestes. Es wäre jedoch falsch, daraus eine absolute Regel abzuleiten, da die nächsten Spiele in Italien 2026, in den USA 2028 und in Frankreich 2030 ganz unterschiedliche Voraussetzungen haben werden. Paris hat den Weg für die Cybersicherheit aufgezeigt und es ist zu hoffen, dass die Schweiz für die Eurovision im Mai 2025 gut gerüstet sein wird. Denn machen wir uns nichts vor, der European Song Contest ist auch eine Riesenveranstaltung, die ebenfalls im Visier verschiedenen bösartigen Akteuren stehen wird.

In Zukunft wird es jedoch auch darum gehen, nicht mehr die fantastischen Zahlen von Milliarden von Angriffen zu verkünden. Denn ein Ping ist kein Cyberangriff. Und wenn ein Dieb die Webseite einer Bank beobachtet, ist das noch kein Raubüberfall...

▶ **Telegram** - Wie sind die Verhaftung von Pavel Durov und die gegen ihn erhobenen

absolute rule from this, as the next Games in Italy in 2026, the USA in 2028 and France in 2030 will all have different conditions. Paris has shown the way in terms of cybersecurity, and we can only hope that Switzerland will be up to the task for Eurovision in May 2025. Make no mistake about it, the European Song Contest is also a giant event, and one that will also be in the crosshairs of various malevolent actors.

In future, however, we'll also have to stop announcing fantastic figures of billions of attacks. After all, a ping is not a cyberattack. And when a thief looks at a bank's web page, it's still not a robbery...

▶ **Telegram** - How to interpret Pavel Durov's arrest and the charges against him. A welcome stop to the cowboy behavior of some tech company bosses who give criminals weapons they shouldn't have, while failing to cooperate (enough) with legitimate state authorities? But if Durov is arrested, what then of Musk, Pichai and Zuckerberg in particular, whose companies are constantly being accused and convicted of not playing by the rules? Is this arrest, on the contrary, a gigantic mistake and an inadmissible attack on freedom of expression and the private sphere? As always, the truth lies in-between, and in any case, the sovereignty of the State cannot be called into question. In Switzerland, too, clarification would be welcome, as we also have

arrestation est-elle au contraire une gigantesque erreur et une attaque inadmissible contre la liberté d'expression et la sphère privée ? Comme toujours, la vérité est au centre et dans tous les cas, la souveraineté de l'État ne saurait être remise en cause. En Suisse aussi une clarification serait la bienvenue, car nous avons aussi des champions tels que Proton, Sharekey ou Threema, dont les services sont essentiels et doivent être promus et protégés.

▶ **Politique énergétique** – Le graphique qui suit (STATISTA) présente la quantité de données créées, capturées, copiées et consommées dans le monde de 2010 à 2020 et les prévisions jusqu'en 2025, le tout exprimé en zettabyte qu'une animation peut rendre accessible, mais attention, le graphique parle lui de 181 ZB ! Certains milieux aiment fustiger le transport aérien, mais qu'en est-il vraiment du numérique en termes de consommation de ressources naturelles et d'énergie ? La stratégie suisse votée en 2015 tient-elle compte de cette évolution, notamment depuis l'explosion de l'usage grand public de l'IA à fin 2022 ? Quel impact sur l'économie suisse dès lors que certaines pénuries vont immanquablement être exacerbées par notre frénésie technologique ? L'absence (visible) de vision politique, d'anticipation et de prospective sur ces thèmes en Suisse interpelle. Pourtant toutes les données sont

Anklagen zu interpretieren? Ein willkommener Stopp für das Cowboy-Verhalten einiger Chefs von Tech-Unternehmen, die Kriminellen Waffen geben, die sie nicht haben sollten, während sie nicht (ausreichend) mit den legitimen Behörden der Staaten zusammenarbeiten? Aber wenn Durov verhaftet wird, was ist dann mit Musk, Pichai und Zuckerberg, deren Unternehmen immer wieder angeklagt und verurteilt werden, weil sie sich nicht an die Regeln halten? Ist diese Verhaftung stattdessen ein grosser Fehler und ein unzulässiger Angriff auf die Meinungsfreiheit und die Privatsphäre? Wie immer steht die Wahrheit im Mittelpunkt und in jedem Fall darf die Souveränität des Staates nicht in Frage gestellt werden. Auch in der Schweiz wäre eine Klärung willkommen, da wir auch Champions wie Proton, Sharekey oder Threema haben, deren Dienstleistungen von wesentlicher Bedeutung sind und gefördert wie auch geschützt werden müssen.

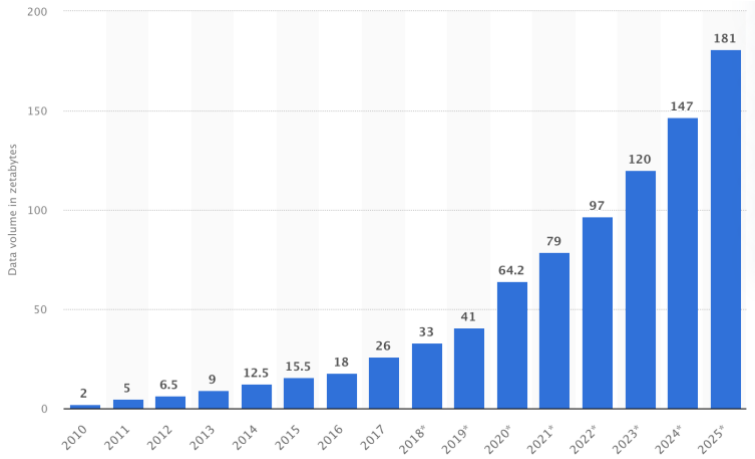
▶ **Energiepolitik** - Die folgende Grafik (STATISTA) zeigt die Menge der weltweit erzeugten, erfassten, kopierten und verbrauchten Daten von 2010 bis 2020 und die Prognosen bis 2025, ausgedrückt in Zettabyte, die durch eine Animation zugänglich gemacht werden können. Aber Vorsicht, die Grafik spricht von 181 ZB! In einigen Kreisen wird gerne der Luftverkehr gegeisselt, aber wie steht es wirklich um

champions such as Proton, Sharekey and Threema, whose services are essential and must be promoted and protected.

▶ **Energy policy** - The following graph (STATISTA) shows the amount of data created, captured, copied and consumed worldwide from 2010 to 2020 and forecasts to 2025, all expressed in zettabytes, which an animation can make accessible. But beware, the graph speaks of 181 ZB! Some circles like to castigate air transportation, but what about digital in terms of consumption of natural resources and energy? Does the Swiss strategy voted on in 2015 take this development into account, particularly since the explosion in consumer use of AI since the end of 2022? What impact will this have on the Swiss economy, given that certain shortages will inevitably be exacerbated by our technological frenzy? The (visible) lack of political vision, anticipation and foresight on these issues in Switzerland is a matter of concern. Yet all the facts are available, including the fact that Microsoft is planning to restart a nuclear reactor at Three Mile Island, and that storm Helene at the end of September is still sending shockwaves through the semiconductor industry after disrupting the supply of quartz sand. Because to make electronic components, you need silicon... An example of the essential systemic view that most decision-makers lack.

disponibles, même le fait que Microsoft envisage de relancer un réacteur nucléaire à Three Mile Island et que la tempête Helene de fin septembre envoie encore des ondes de choc dans l'industrie des semi-conducteurs après avoir provoqué une rupture de l'approvisionnement de sable de quartz. Car pour faire des composants électroniques, il faut du silicium… Un exemple de l'indispensable vue systémique qui manque à une majorité de décideurs.

die Digitalisierung in Bezug auf den Verbrauch von natürlichen Ressourcen und Energie? Berücksichtigt die 2015 verabschiedete schweizerische Strategie diese Entwicklung, insbesondere seit der explosionsartigen Zunahme der Nutzung von KI durch die Allgemeinheit bis Ende 2022? Wie wird sich dies auf die Schweizer Wirtschaft auswirken, wenn bestimmte Knappheiten unweigerlich durch unseren Technologiewahn verschärft werden? Das (sichtbare) Fehlen einer politischen Vision, einer Antizipation und einer vorausschauenden Planung zu diesen Themen in der Schweiz ist beunruhigend. Dabei sind alle Daten verfügbar, sogar die Tatsache, dass Microsoft die Wiederinbetriebnahme eines Atomreaktors auf Three Mile Island plant und dass der Sturm Helene Ende September immer noch Schockwellen in der Halbleiterindustrie auslöst, nachdem er zu einer Unterbrechung der Quarzsandversorgung geführt hat. Ein Beispiel für die notwendige systemische Sichtweise, die einer Mehrheit der Entscheider fehlt.



▶ Divers aux USA – On pourrait écrire un roman sur les multiples attaques dont souffrent les USA en lien avec l'élection présidentielle, notamment au travers des médias sociaux. Pour l'instant, contentons-nous d'observer, les techniques, tactiques et procédures (TTP's) des attaquants qui trouveront tôt ou tard le chemin de l'Europe et de la Suisse. Dans ce cadre, Russes et Iraniens jouent un rôle considérable. Les premiers sont déjà connus en Suisse et nous serions bien inspirés de ne pas sous-estimer les seconds. On ne le dit pas assez – surtout on n'agit pas assez – les menaces pour la démocratie et la culture occidentale sont immenses.

Le FBI a annoncé avoir déjoué d'importantes attaques chinoises visant les infrastructures critiques alors que les grues d'origine chinoise équipant les ports maritimes sont accusées de disposer de portes dérobées et que les universités commencent à s'inquiéter quant à certains étudiants qui aident la Chine à contourner

▶ Verschiedenes in den USA – Man könnte einen Roman über die zahlreichen Angriffe schreiben, denen die USA im Zusammenhang mit der Präsidentschaftswahl ausgesetzt sind, insbesondere über die sozialen Medien. Für den Moment begnügen wir uns damit, die Techniken, Taktiken und Verfahren (TTP's) der Angreifer zu beobachten, die früher oder später ihren Weg nach Europa und in die Schweiz finden werden. In diesem Zusammenhang spielen Russen und Iraner eine wichtige Rolle. Erstere sind in der Schweiz bereits bekannt und wir sind gut beraten, die Letzteren nicht zu unterschätzen. Es wird nicht genug gesagt – und vor allem nicht genug getan –, dass die Bedrohungen für die Demokratie und die westliche Kultur immens sind.

Das FBI gab bekannt, dass es grosse chinesische Angriffe auf kritische Infrastrukturen vereitelt hat, während chinesische Kräne in Seehäfen beschuldigt werden, Hintertüren zu haben, und die

▶ Miscellaneous in the USA – One could write a novel on the multiple attacks suffered by the USA in connection with the presidential election, particularly through social media. For now, let's content ourselves with observing the techniques, tactics and procedures (TTP's) of the attackers who will sooner or later find their way to Europe and Switzerland. In this context, the Russians and Iranians play a considerable role. The former are already well known in Switzerland, and we would be well advised not to underestimate the latter. We don't say it enough - and, above all, we don't do enough about it - the threats to democracy and Western culture are immense.

The FBI has announced that it has thwarted major Chinese attacks on critical infrastructures, while cranes of Chinese origin used in seaports are accused of having backdoors, and universities are beginning to worry about certain students who are

par la voie académique, les restrictions imposées pour des raisons de sécurité nationale. Nouveau ? Absolument pas, mais la même question revient de façon insistante: que fait-on chez nous de ces observations ? Doit-on, pour enfin agir, répéter les mêmes erreurs ?

La Maison Blanche vient par ailleurs de publier un projet pour interdire les logiciels chinois dans les voitures. Lubie protectionniste américaine ? Non, si on se base sur les nombreux cas que nous avons aussi rapportés dans de précédentes éditions de cette newsletter.

Universitäten beginnen, sich über einige Studenten Sorgen zu machen, die China helfen, die aus Gründen der nationalen Sicherheit auferlegten Beschränkungen auf akademischem Wege zu umgehen. Ist das neu? Absolut nicht, aber es stellt sich immer wieder die gleiche Frage: Was wird mit diesen Beobachtungen bei uns gemacht? Müssen wir, um endlich zu handeln, die gleichen Fehler wiederholen?

And finally… das Weisse Haus hat einen Entwurf veröffentlicht, um chinesische Software in Autos zu verbieten. Eine protektionistische List der USA? Bestimmt nicht, wenn man die vielen Fälle betrachtet, über die wir in früheren Ausgaben dieses Newsletters berichtet haben.

helping China to circumvent restrictions imposed for national security reasons through academic channels. New? Not at all, but the same question keeps coming up: what do we do with these observations? Do we have to repeat the same mistakes?

And last but not least… the White House has just published a plan to ban Chinese software in cars. Is this an American protectionist ploy? Surely not, based on the numerous cases we have also reported in previous editions of this newsletter.

Voilà pour cette 105ème édition. Nous espérons qu'elle vous a, une fois encore, inspiré et vous souhaitons une enrichissante découverte des articles et liens sélectionnés.

Das war's für diese 105. Ausgabe. Wir hoffen, dass sie Sie einmal mehr inspiriert hat und wünschen Ihnen viele Erkenntnisse bei den ausgewählten Artikel und Links.

That's all for this 105th edition. We hope you enjoyed it again and wish you an enriching discovery of the selected articles and links.

Merci également de souscrire à *d*VPedia et ainsi de soutenir son développement au profit de tous.

Bitte registrieren Sie sich ebenfalls für *d*VPedia und unterstützen Sie damit seine Entwicklung zum Nutzen aller.

Thank you for subscribing to *d*VPedia and supporting its development for the benefit of all.

Merci de penser à soutenir *digi*Volution.	Bitte denken Sie daran, *digi*Volution zu unterstützen.	Please consider supporting *digi*Volution.

digiVolution

TWINT

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.
Ce billet est rédigé par des individus et non par de l'IA. Nous employons des moyens techniques utilisant de l'IA pour soutenir nos recherches, mais ne lui confions aucune tâche rédactionnelle ou de réflexion.

Seit dem 8. Januar 2021 veröffentlicht digiVolution regelmässig Newsletter, die von einer Auswahl «handverlesener» Artikel begleitet wird, die die Komplexität, der mit der digitalen Mutation einhergehenden Herausforderungen veranschaulichen; Sie finden diese unter https://www.digivolution.swiss/dv-blog.
Dieser Beitrag wird von Menschen und nicht von KI geschrieben. Wir setzen technische Mittel ein, die KI verwenden, um unsere Forschung zu unterstützen, übertragen KI jedoch keine redaktionellen oder gedanklichen Aufgaben.

Since January 8, 2021, digiVolution has been publishing a newsletter that accompanies a selection of «hand picked» articles to illustrate the complexity of the challenges linked to digital mutation; they are available at https://www.digivolution.swiss/dv-blog.
This newsletter is written by individuals, not by AI. We employ technical means using AI to support our research, but do not entrust it with any editorial or reflective tasks