

Les billetsⁱ de *digiVolution* / *digiVolution's* Newsletters
[23.05.2022 - 51^{ème} édition]

BACYSEC

Chers Lectrices et Lecteurs

Voici les **dV-News 11-2022** et leur sélection d'[articles et de liens](#) pour illustrer l'actualité de la dernière quinzaine. Dans cette édition, nous nous arrêterons à nouveau sur l'Ukraine (impossible d'y échapper), l'avenir des mots de passe, la confiance et les récents développements à Berne, notamment la décision de créer un office fédéral dédié à la cybersécurité. Osons un acronyme: le **BACYSEC**? Bundesamt für CyberSecurity?

Cyber in War (suite et pas fin)

A deux heures de vol de Zürich, la guerre continue à faire rage, même si la baisse de contributions sur ce sujet dans les médias trahit déjà un début de fatigue des commentateurs et du public. Ne nous leurrions pas, la situation en Ukraine reste dramatique et les risques de dérapages de toutes sortes demeurent. Pour ceux qui pensent que cette guerre n'a pas atteint l'envergure attendue dans le cyberspace, le général [Nakasone](#) - patron de la NSA et du US Cyber Command - s'est exprimé à son tour clairement sur le sujet il y a quelques jours, estimant que ceux qui raillaient l'absence relative de cyberagressions russes en dehors de l'Ukraine parlent trop tôt. Comme nous ne cessons de le répéter chez *digiVolution*, ne baissons pas la garde, car cela ne fait que de commencer et prenons les dispositions préventives nécessaires. L'exemple du [Costa Rica \(lire aussi\)](#) devant déclarer l'état d'urgence devrait nous inspirer. Et n'oublions pas que le temps des plateaux télé n'est pas

Liebe Leserinnen und Leser

Dies sind die **dV-News 11-2022** und unsere Auswahl von [Artikeln und Links](#), die die Nachrichten der letzten zwei Wochen aufzeigen. In dieser Ausgabe beschäftigen wir uns erneut mit der Ukraine (an der man nicht vorbeikommt), der Zukunft von Passwörtern, Vertrauen und den jüngsten Entwicklungen in Bern, insbesondere dem Beschluss, ein Bundesamt für Cybersicherheit zu schaffen. Lassen Sie uns ein Akronym riskieren: das **BACYSEC**? Bundesamt für CyberSecurity?

Cyber in War (Fortsetzung und nicht Ende)

Zwei Flugstunden von Zürich entfernt tobt der Krieg weiter, auch wenn der Rückgang der Beiträge zu diesem Thema in den Medien bereits auf eine beginnende Ermüdung der Kommentatoren und der Öffentlichkeit hindeutet. Machen wir uns nichts vor, die Lage in der Ukraine ist nach wie vor dramatisch und die Gefahr von Entgleisungen aller Art bleibt bestehen. Für diejenigen, die der Meinung sind, dass dieser Krieg im Cyberraum nicht das erwartete Ausmass erreicht hat, hat sich General [Nakasone](#) - Chef der NSA und des US Cyber Command - vor einigen Tagen ebenfalls deutlich zu diesem Thema geäußert und meint, dass diejenigen, die sich über die relative Abwesenheit russischer Cyberaggressionen ausserhalb der Ukraine lustig machen, zu früh freuen. Wie wir bei *digiVolution* immer wieder betonen, sollten wir nicht nachlassen, denn es hat gerade erst begonnen, und die notwendi-



celui du [terrain](#)...! Dans notre précédent billet, nous parlions de [\(N\)NEMP](#)? Eh bien le [soleil](#) a déjà brûlé la politesse à M. Poutine en nous gratifiant le 10 mai dernier d'une énergique piquûre de rappel.

La fin des mots de passe?

Apple, Google et Microsoft nous annoncent la fin [des mots de passe](#). Certains se réjouissent, mais pas nous. Ce que ces géants annoncent comme un *progrès* va conduire à une nouvelle perte de souveraineté et de liberté des individus. Ce sera certes très pratique de ne plus avoir de Sésame à définir (autre que 123456...), à mémoriser, à protéger dans un petit carnet, ou dans un gestionnaire crypté ou avec un Post-it sous son clavier (ceci est une blague) mais il y a un gros "mais". Tout passera désormais principalement par notre smartphone et la [captation des consommateurs](#) par les plateformes des géants de la tech - des États dans les États - sera ainsi complète et définitive. Demain sera peut-être moins compliqué pour le consommateur, mais à quel prix? Les bien-pensants européens se moquent de la Chine et de son système de crédit social, pourtant nous empruntons à marche forcée le même chemin qui consiste à vouloir tout régenter par la technologie en s'appuyant sur [de l'IA](#) que l'on nourrit désormais avec des [données synthétiques](#) pour apprendre à détecter nos réactions. La démocratie et la liberté peuvent trembler. Au travers de sa lutte - légitime - contre la pédopornographie, l'[UE](#) risque fort d'y contribuer et d'ouvrir des portes insoupçonnées que ne pourront plus être refermées.

La confiance dans le cyberspace

Puis-je avoir confiance qu'un produit TIC matériel ou logiciel a été développé de manière à le mettre à l'abri de menaces [internes](#) ou externes à l'organisation? Puis-je être certain que les fabricants des composants ne se sont pas octroyé une porte dérobée à leur avantage et au détriment de leurs clients? Quelles protections politiques et légales sont en place pour permettre aux clients de se retourner contre

gen Vorsichtsmassnahmen treffen. Das Beispiel von [Costa Rica](#) ([auch lesen](#)), das den Notstand ausrufen musste, sollte uns Warnung genug sein. Und vergessen wir nicht, dass der Faktor Zeit der Fernsehberichte nicht unbedingt dasjenige vom [Feld](#) darstellt...! In unserem letzten Newsletter sprachen wir über [\(N\)NEMP](#)? Nun, die [Sonne](#) hat Herrn Putin bereits den Rang abgelaufen, indem sie uns am 10. Mai mit einem energievollen Reminder beglückte.

Das Ende der Passwörter?

Apple, Google und Microsoft verkünden das Ende der Passwörter. Manche freuen sich darüber, wir nicht. Was diese Giganten als Fortschritt ankündigen, wird zu einem weiteren Verlust der Souveränität und der Freiheit des Einzelnen führen. Es wird zwar sehr praktisch sein, kein Sesam-öffne-dich mehr zu definieren (diesmal nicht 123456...), sich zu merken, in einem kleinen Notizbuch zu schützen, in einem verschlüsselten Manager oder mit einem Post-it unter seiner Tastatur (das ist ein Witz) zu «verbergen» es gibt ein grosses "aber". Alles wird künftig hauptsächlich über unser Smartphone laufen und die [Vereinnahmung der Konsumenten](#) durch die Plattformen der Tech-Giganten - Staaten in Staaten - wird damit vollständig und endgültig sein. Das Morgen mag für den Konsument weniger kompliziert sein, aber zu welchem Preis? Die europäischen Besser-Wisser machen sich über China und sein Sozialkreditsystem lustig, aber wir gehen mit Vollgas denselben Weg, der darin besteht, alles durch Technologie regeln zu wollen, indem wir uns auf [KI](#) stützen, die wir nun mit [synthetischen Daten](#) füttern, um zu lernen, unsere Reaktionen zu erkennen. Die Demokratie und die Freiheit können zittern. Durch ihren - legitimen - Kampf gegen Kinderpornografie wird die [EU](#) wahrscheinlich dazu beitragen und ungeahnte Türen öffnen, die nicht mehr geschlossen werden können.

Vertrauen im Cyberraum

Kann ich darauf vertrauen, dass ein IKT-Hardware- oder Softwareprodukt so entwickelt



des prestataires indécents. La [NSA jure](#) que cette fois elle ne mettra pas de porte dérobée dans les prochains standards de cryptographie quantique. Nous voilà rassurés..., mais pour bien appréhender le problème nous vous recommandons ce passionnant [rapport du Lawfare Institute "Trusted Hardware and Software Working Group"](#) sur le sujet de la confiance. Une autre démarche que nous pouvons recommander peut être déduite des nouvelles [directives de la Présidence US](#) qui montrent que la cybersécurité tient souvent plus de la simple mise en œuvre des meilleures pratiques connues dans le monde réel que d'hypothétiques murs de protection technique tous azimuts. Toujours les bonnes vieilles recettes, bientôt soutenues on l'espère par une [convention internationale sur la cybercriminalité](#) sous l'égide de l'ONU.

wurde, dass es vor Bedrohungen [innerhalb](#) oder ausserhalb der Organisation geschützt ist? Kann ich sicher sein, dass die Hersteller der Komponenten keine Hintertür zu ihrem eigenen Vorteil und zum Nachteil ihrer Kunden eingebaut haben? Welche politischen und rechtlichen Schutzmassnahmen gibt es, damit Kunden gegen unzuverlässige Anbieter vorgehen können? Die [NSA schwört](#), dass sie diesmal keine Hintertüren in die nächsten Standards für Quantenkryptologie einbauen wird. Damit sind wir beruhigt..., aber um das Problem richtig zu verstehen, empfehlen wir Ihnen diesen spannenden [Bericht vom Lawfare Institute "Trusted Hardware and Software Working Group"](#) zum Thema Vertrauen. Ein weiterer Ansatz, den wir empfehlen, lässt sich aus den neuen [Richtlinien der US-Präsidentschaft](#) ableiten, die zeigen, dass es bei der Cybersicherheit oft mehr um die einfache Umsetzung von Best Practices aus der realen Welt geht als um hypothetische technischen Schutzmauern in alle Richtungen. Es sind immer noch die alten Rezepte, die hoffentlich bald durch eine [internationale Konvention zur Cyberkriminalität](#) unter der Schirmherrschaft der Vereinten Nationen unterstützt werden.



Mission accomplie

Il y a 10 ans, André Duillard devenait Délégué du Réseau national de sécurité (RNS) et arrivait à Berne dans un bureau vide et tout à créer. A

Auftrag erfüllt

Vor zehn Jahren wurde André Duillard Delegierter des Sicherheitsverbunds Schweiz (SVS) und kam in Bern in ein leeres Büro, wo alles neu zu schaffen war. Ende Juli wird er seinem



fin juillet il remettra définitivement à son successeur, Martin von Muralt, les clefs d'un RNS qui a très largement contribué à améliorer la collaboration entre les acteurs de la sécurité en Suisse avec une recette simple: le dialogue et le respect. Merci, M. Duvillard pour vos multiples actions au profit de la sécurité de la Suisse et tous nos vœux à M. von Muralt face aux défis qui se profilent et qui réclameront sans aucun doute de sa part de nouvelles réponses. Bravo aussi pour la 5ème [conférence du RNS](#) et merci d'avoir confié à *digi*Volution la modération du podium consacré au thème "La mobilité génère des données". Ce fut une enrichissante discussion autour de la difficulté à placer le curseur judicieusement entre la protection des personnes, l'usage de leurs données par les acteurs économiques et la capacité de l'État de droit à faire respecter ses règles.

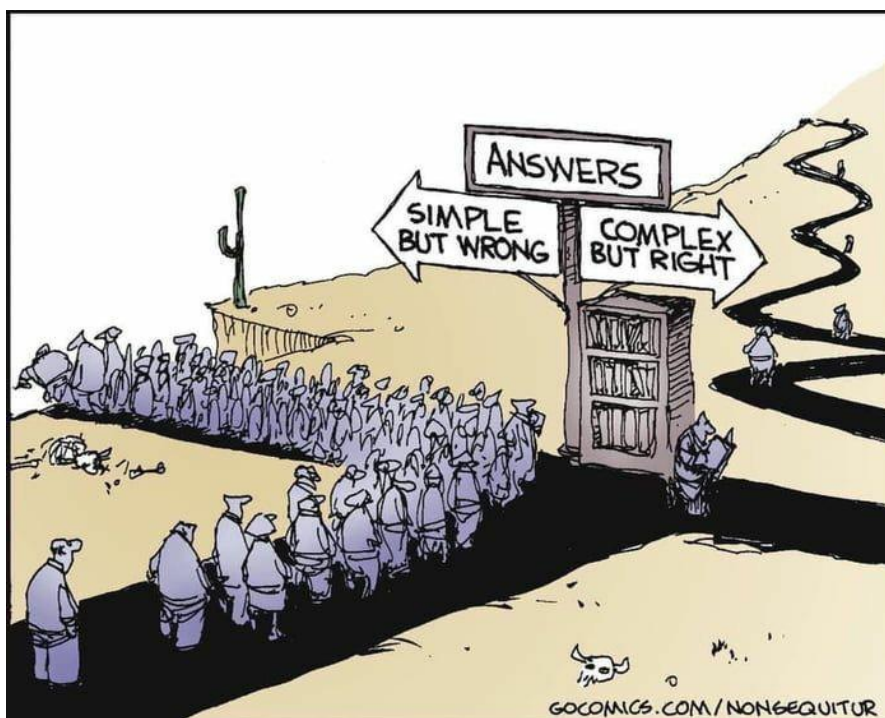
BACYSEC. Enfin !

Lors de l'élaboration de la première stratégie pour la protection de la Suisse contre les cyberrisques en 2012, l'équipe de projet avait proposé la création d'un centre de compétence. L'idée fut balayée de l'intérieur. En 2015 une idée similaire subissait le même sort. En 2016, le Conseil fédéral s'opposait à la motion de la Conseillère nationale Glanzmann et ce n'est qu'en 2017 que le Conseiller aux États Eder parvenait à imposer l'idée d'un centre fédéral de compétence qui fut finalement créé en 2020, avec cependant des moyens ridicules par rapport à l'ampleur de la tâche. Avec la création d'un office fédéral qu'il conviendra encore de définir, de rattacher au bon endroit et auquel il s'agira d'attribuer des moyens en relation avec ses tâches vitales pour la Suisse, une étape clé est franchie. Que de temps perdu... mais un grand bravo à Florian Schütz, architecte de ce progrès. Un chemin rude et exigeant en perspective pour tous, mais enfin le bon.

Nachfolger Martin von Muralt endgültig die Schlüssel des SVS übergeben. André Duvillard hat mit einem einfachen Rezept - dem Dialog und Respekt - viel dazu beigetragen, die Zusammenarbeit zwischen den Sicherheitsakteuren in der Schweiz zu verbessern. Vielen Dank, Herr Duvillard, für Ihre zahlreichen Aktivitäten zugunsten der Sicherheit der Schweiz und alles Gute an Herrn von Muralt angesichts der Herausforderungen, die sich abzeichnen und die zweifellos neuen Antworten von ihm verlangen werden. Gratulation and die 5. [SVS-Konferenz](#) und vor allem vielen Dank dafür, dass *digi*Volution mit der Moderation des Podiums zum Thema "Mobilität generiert Daten" betraut wurde. Es war eine bereichernde Diskussion über die Schwierigkeit, den Cursor sinnvoll zwischen dem Schutz der Menschen, der Nutzung ihrer Daten durch die Wirtschaftsakteure und der Fähigkeit des Rechtsstaats, seine Regeln durchzusetzen, zu platzieren.

BACYSEC. Endlich!

Bei der Ausarbeitung der ersten Strategie zum Schutz der Schweiz vor Cyberrisiken im Jahr 2012 hatte das Projektteam die Schaffung eines Kompetenzzentrums vorgeschlagen. Die Idee wurde von innen heraus weggefeht. Im Jahr 2015 erlitt eine ähnliche Idee das gleiche Schicksal. 2016 lehnte der Bundesrat die Motion von Nationalrätin Glanzmann ab, und erst 2017 gelang es Ständerat Eder, die Idee eines Bundeskompetenzzentrums durchzusetzen, das erst im Jahr 2020 geschaffen wurde, allerdings mit Mitteln, die im Vergleich zum Umfang der Aufgabe lächerlich waren. Mit der Schaffung eines Bundesamtes, das noch definiert und am richtigen Ort angesiedelt werden muss und dem die Mittel im Zusammenhang mit den für die Schweiz lebenswichtigen Aufgaben zugewiesen werden müssen, ist ein entscheidender Schritt getan. Viel Zeit ist verloren gegangen... aber ein grosses Lob an Florian Schütz, den Architekten dieses Fortschritts. Ein harter und anspruchsvoller Weg liegt vor uns, aber endlich der richtige.



Nous vous souhaitons une enrichissante découverte des [articles et liens](#) sélectionnés et nous réjouissons de vous retrouver dans 15 jours.

Bis dahin wünschen wir Ihnen eine bereichernde Entdeckung der ausgewählten [Artikel und Links](#) und freuen uns darauf, Sie in zwei Wochen wieder zu informieren.

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. Ces articles 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. Diese Artikel finden Sie unter <https://www.digivolution.swiss/dv-blog/>. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.