Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[12.10.2023 – Édition / Ausgabe Nr. 86]

Time to join *d*VPedia Pro

Chers Lectrices et Lecteurs

Voici les *d*V-News 20-2023 et leur sélection d'articles et liens.

Merci à celles et ceux qui après le billet consacré à la naissance de *d*VPedia ont déjà fait le pas de s'inscrire à sa version BASICS. La communauté augmente régulièrement.

Depuis nous avons aussi activé *d*VPedia PRO qui offre des prestations uniques qui seront graduellement complétées. Dans cette version *d*VTopics offre p.ex. toutes les fonctionnalités et avec *d*VAssist, nos abonnés bénéficient d'un premier soutien en cas de question. Central à l'heure où les PME sont les grandes perdantes face à la cybercriminalité.

Les cyberrisques et la mutation numérique constituent un défi particulier pour les PME ainsi que pour les cantons et les communes. En conséquence *digi*Volution met, depuis sa création, l'effort principal sur leurs décideurs.

Pour renforcer cet accent et offrir aux décideurs des prestations plus ciblées, le billet bihebdomadaire de *digi*Volution deviendra plus générique et un billet spécifiquement dédié aux décideurs renforcera l'offre de *d*VPedia PRO.

Plus il y aura d'abonnés et meilleure sera notre capacité à vous servir. Merci d'y souscrire et d'en parler autour de vous.

Liebe Leserinnen und Leser

Hier sind die *d*V-News 20-2023 und eine Auswahl an Artikeln und Links.

Vielen Dank an alle, die nach dem Beitrag über die Geburt von *d*VPedia bereits den Schritt gewagt haben, sich für die BASICS-Version zu registrieren. Die Gemeinschaft wächst stetig.

Seitdem haben wir ebenfalls *d*VPedia PRO aktiviert, das einzigartige Leistungen bietet, die schrittweise erweitert werden. In dieser Version bietet zB *d*VTopics alle Funktionen und mit *d*VAssist erhalten unsere Abonnenten bereits einen ersten Support, wenn sie Fragen haben. Zentral in einer Zeit, in der KMUs die grössten Verlierer der Cyberkriminalität sind.

Cyberrisiken und die digitale Mutation stellen eine besondere Herausforderung für KMU's sowie für Kantone und Gemeinden dar. Daher konzentriert sich *digi*Volution seit seiner Gründung auf deren Entscheider.

Um diesen Schwerpunkt zu verstärken und Entscheidungsträgern gezieltere Leistungen anzubieten, wird der zweiwöchentliche *digi*Volution -Newsletter generischer und ein speziell auf Entscheidungsträger ausgerichteter Beitrag wird das Angebot von *d*VPedia PRO erweitern.

Je mehr Abonnenten, desto besser können wir Sie bedienen. Bitte abonnieren Sie sich und erzählen Sie es weiter.

Parmi les informations découvertes pour l'élaboration de ce billet, deux ont particulièrement retenu notre attention.

- Monsieur Hans de Vries, directeur du centre national de cybersécurité au ministère néerlandais de la Justice et de la Sécurité était interrogé sur les leçons de la guerre en Ukraine. Il relève que jusqu'ici la guerre n'a pas (encore?) été un facteur d'aggravation en matière de cyberrisques contre les infrastructures critiques hollandaises. Il observe aussi que face à un événement grave comme la guerre en Ukraine, les organisations commerciales font preuve d'une plus grande agilité que l'État pour s'adapter à la situation, leurs processus décisionnels étant plus rapides. Il relève enfin qu'en cas de conflit, une infrastructure cloud représente un avantage, puisque les données sont dispersées hors du périmètre des opérations. S'agissant de l'apport du secteur privé, il salue celui de Starlink. Sur ce point nous sommes d'accord, mais avec la (très grosse) réserve quant au rôle politique des entreprises que nous avons discuté dans notre billet du 12 septembre dernier.
- Le second sujet qui nous a interpellés, c'est la tendance croissante des États à se tourner vers une forme proactive de la cyberdéfense, consistant à combattre préventivement les cybermalveillants pour les empêcher de mener à bien leurs actions. Le long et passionnant article de la Stiftung für Wissenschaft und Politik sur le changement de paradigme dans la cyberdéfense européenne ainsi que l'article de Chatham House contribuent utilement à une discussion importante et nécessaire sur un sujet sensible. Dans ce cadre, il est utile de considérer également la discussion entre l'UE et l'OTAN sur une coopération renforcée en matière de cyberdéfense. Si les actions préventives devenaient la règle, le cyberespace se transformerait alors en une sorte de vaste terrain de conflit avec des violations systématique de la souveraineté des États et des questions sans fin d'attribution et

Von den Informationen, die wir für diesen Beitrag entdeckt haben, sind uns zwei besonders aufgefallen.

- Zuerst wurde Herr Hans de Vries, Direktor des nationalen Zentrums für Cybersicherheit im niederländischen Ministerium für Justiz und Sicherheit, unsere Aufmerksamkeit über die Auswirkungen des Krieges in der Ukraine gefragt. Für ihn war der Krieg bisher (noch?) kein Faktor, der die Cyberrisiken für kritische Infrastrukturen in den Niederlanden erhöht hat. Er stellt ebenfalls fest, dass kommerzielle Organisationen bei einem schwerwiegenden Ereignis wie dem Krieg in der Ukraine eine grössere Agilität als der Staat zeigen, um sich an die Lage anzupassen, da ihre Entscheidungsprozesse schneller sind. Er wies zuletzt auch darauf hin, dass eine Cloud-Infrastruktur im Falle eines Konflikts von Vorteil ist, da die Daten ausserhalb des Operationsgebiets verstreut werden. In Bezug auf den Beitrag des Privatsektors begrüsst er Starlink. Hier stimmen wir zu, jedoch mit dem (sehr grossen) Vorbehalt bezüglich der politischen Rolle der Unternehmen, den wir in unserem Beitrag vom 12. September diskutiert haben.
- Das zweite Thema, das uns beschäftigte, ist die zunehmende Tendenz der Staaten, sich einer proaktiven Form der Cyberdefence zuzuwenden, die darin besteht, Cyberkriminelle präventiv zu bekämpfen, um sie an der Durchführung ihrer Aktionen zu hindern. Der lange und spannende Artikel der Stiftung für Wissenschaft und Politik über den Paradigmenwechsel in der europäischen Cyberabwehr sowie der Artikel von Chatham House sorgen für eine wichtige und notwendige Diskussion zu einem sensiblen Thema. In diesem Zusammenhang ist es nützlich, auch die Diskussion zwischen der EU und der NATO über eine verstärkte Zusammenarbeit im Bereich der Cyberdefence zu betrachten. Wenn präventive Massnahmen zur Regel werden, würde sich der Cyberraum in eine Art grosses Konfliktfeld verwandeln, mit systematischen

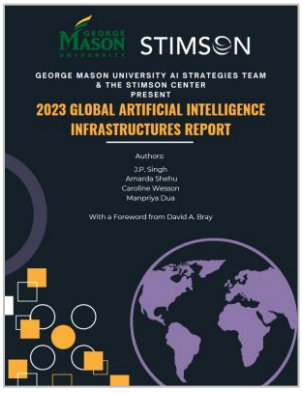
d'identification des acteurs malveillants et de leurs intentions. Et quid des actions contre de tels acteurs si ceux-ci vont se dissimuler dans des infrastructures – logiques ou physiques – utilisées par des services et utilisateurs légitimes? Les USA appellent ces actions des *Hunt-Forward-Operations* (HFO), mais qui peut se les permettre? La loi du plus fort s'appliquerait donc ici? Cette tendance à la réponse violente nous paraît démontrer l'impuissance croissante de la communauté internationale à trouver des solutions à l'augmentation inéluctable des dégâts dans le cyberespace, une situation qui découle en grande partie de l'intérêt des grandes puissances à maintenir un «*status quo d'insécurité par dessin*». Alors que la guerre en Ukraine a déjà conduit des deux côtés à la violation de toutes les règles du Droit International Humanitaire dans le domaine cyber, nous encourageons à considérer la proposition de deux experts du CICR sur des règles de comportement pour les hackers civils en temps de guerre.

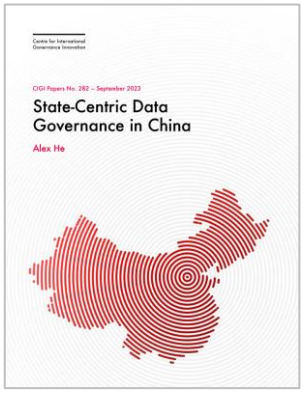
Verletzungen der staatlichen Souveränität und endlosen Fragen der Attribution und Identifizierung von böswilligen Akteuren und ihren Absichten. Und was ist mit Aktionen gegen solche Akteure, wenn diese sich in – logischen oder physischen – Infrastrukturen verstecken, die von legitimen Diensten und Nutzern verwendet werden? Die USA nennen solche Aktionen *Hunt-Forward-Operations* (HFO), aber wer kann sich das leisten? Gilt hier also das Recht des Stärkeren? Diese Tendenz zu gewalttätigen Reaktionen scheint uns die wachsende Hilflosigkeit der internationalen Gemeinschaft bei der Suche nach Lösungen für die unausweichliche Zunahme von Schäden im Cyberraum zu zeigen, eine Situation, die zum grossen Teil auf das Interesse der Grossmächte zurückzuführen ist, ihren «*Status quo der Unsicherheit by Design*» aufrechtzuerhalten. Da der Krieg in der Ukraine bereits auf beiden Seiten zur Verletzung aller Regeln des humanitären Völkerrechts im Cyberbereich geführt hat, möchten wir Sie ermutigen, den Vorschlag zweier Experten des IKRK über Verhaltensregeln für zivile Hacker in Kriegszeiten in Erwägung zu ziehen.

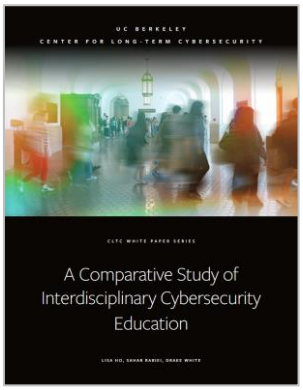
BOOKS & REPORTS

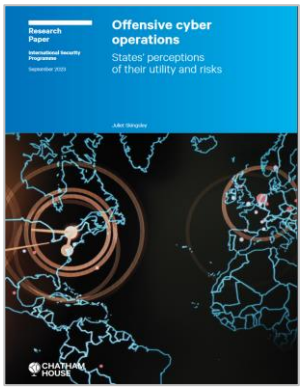
Voici les livres et publications d'intérêts découverts durant nos recherches des dernières deux semaines. Pour rappel, ne souhaitant pas faire de la promotion pour les quelques éditeurs que ce soit quand il s'agit d'ouvrages commerciaux, nous vous laissons trouver le distributeur qui vous convient.

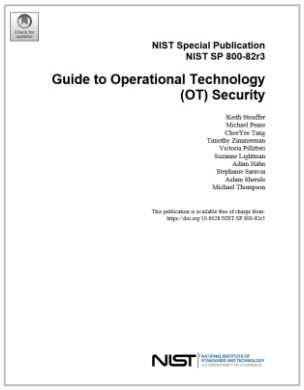
Hier sind die Bücher und Publikation von Interesse, die wir bei unseren Recherchen in den letzten zwei Wochen gefunden haben. Wir möchten Sie daran erinnern, dass wir bei kommerziellen Büchern nicht für einen Verlag werben möchten und überlassen es Ihnen, den für Sie passenden Händler zu finden.











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

- Le 25 septembre dernier, nous avons pu observer un phénomène très inhabituel en Suisse: une aurore boréale. Cet événement doit nous rappeler que le soleil connaît de manière cyclique de gigantesques tempêtes dont les effets peuvent s'avérer catastrophiques pour les équipements électriques et informatiques sur et autour de la Terre. Un thème que nous remettons régulièrement, à l'ordre du jour alors que la prochaine crise solaire majeure est prévue pour juillet 2025.

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

- Am 25. September konnten wir in der Schweiz ein sehr ungewöhnliches Phänomen beobachten: das Nordlicht. Dieses Ereignis muss uns daran erinnern, dass die Sonne zyklisch riesige Stürme erzeugt, die katastrophale Auswirkungen auf die elektrische und informationstechnische Ausrüstung auf und um die Erde haben können. Ein Thema, das wir regelmässig auf die Tagesordnung setzen, da die nächste grosse Sonnenkrise für Juli 2025 vorhergesagt ist.

- Les **cybermercenaires**, un fléau croissant. Lors de l'élection de Donald Trump en 2016, les prouesses de Cambridge Analytica avaient finalement précipité en 2018 sa perte, mais une tendance était lancée.

- **Cybersöldner**, eine wachsende Plage. Bei der Wahl von Donald Trump im Jahr 2016 führten die Leistungen von Cambridge Analytica schliesslich zu dessen Niederlage im Jahr 2018, aber ein Trend wurde

Celle-ci a été observée lors du BREXIT, mais le gouvernement britannique a préféré enterrer le rapport de ses services de renseignement. Plus récemment, un intéressant documentaire a été produit sur une firme israélienne, le Team Jorge qui aurait influencé 33 votes et élections, principalement en Afrique, dont 27 fois avec succès. Ce sont ces agissements qui mettent en péril le modèle démocratique et qu'analyse l'intéressant rapport du Quad, l'alliance entre les USA, l'Australie, l'Inde et le Japon pour contrer les actions d'influence de la Chine.

Nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés et nous réjouissons de vous retrouver bientôt.

eingeleitet. Dieser war auch beim BREXIT zu beobachten, aber die britische Regierung zog es vor, den Bericht ihres Nachrichtendienstes zu begraben. In jüngster Zeit wurde ein interessanter Dokumentarfilm über eine israelische Firma, Team Jorge, produziert, die angeblich 33 Abstimmungen und Wahlen, hauptsächlich in Afrika, beeinflusst haben soll, 27 Mal davon erfolgreich. Es sind diese Handlungen, die das demokratische Modell gefährden und die in dem interessanten Quad-Bericht analysiert werden, die Allianz zwischen den USA, Australien, Indien und Japan, um Chinas Einflussnahme zu begegnen.

Wir wünschen Ihnen viele lehrreiche Entdeckungen in 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 https://www.digivolution.swiss/dv-blog. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.*