Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[11.10.2022 – 61ème édition]

CIP

Chers Lectrices et Lecteurs

Voici les ***d*V-News 21-2022** et leur sélection d'articles et de liens pour illustrer l'actualité de la dernière quinzaine. Cette édition comporte quatre volets: une réflexion sur la protection des infrastructures critiques (CIP), notre revue de la cyberactualité internationale, une rubrique spéciale «Books» et l'actualité en Suisse.

Liebe Leserinnen und Leser

Dies sind die ***d*V-News 21-2022** und unsere Auswahl von Artikel und Links, die die Nachrichten der letzten zwei Wochen aufzeigen. Diese Ausgabe ist in vier Teile gegliedert: eine Überlegung über den Schutz kritischer Infrastrukturen (CIP), unsere Übersicht über die internationale Cyberaktualität, eine Sonderrubrik «Books» und aktuelle Nachrichten aus der Schweiz.

Mais commençons par un grand coup de chapeau pour l'élection de Mme Doreen Bogdan-Martin à la tête de l'UIT. Victoire sans appel : 139 à 33 contre le candidat russe. Et première femme à la tête de cette institution vieille de 157 ans.

Beginnen wir jedoch mit einem grossen Lob für die Wahl von Frau Doreen Bogdan-Martin zur ITU-Chefin. Eindeutiger Sieg: 139 zu 33 gegen den russischen Kandidaten. Und die erste Frau an der Spitze dieser 157 Jahre alten Institution.

Les infrastructures vitales en danger

L'acronyme CIP (Critical Infrastructure Protection) faisait le bonheur des chercheurs au début des années 2000. Avec le développement numérique, une branche s'était développée, le CIIP, avec ce «I» supplémentaire pour «information infrastructure». Un thème alors particulièrement bien couvert par l'ETHZ avec le CIIP Handbook, mais un effort qui s'est malheureusement interrompu en 2008.

Kritische Infrastrukturen in Gefahr

Das Akronym CIP (Critical Infrastructure Protection) war in den frühen 2000er Jahren ein beliebtes Feld für Forscher. Mit der digitalen Entwicklung entwickelte sich ein eigener Zweig, CIIP, mit dem zusätzlichen «I» für «Information Infrastructure». Dieses Thema wurde damals von der ETHZ mit dem CIIP Handbook besonders gut abgedeckt, wobei diese Bemühungen 2008 leider eingestellt wurden.

Que lirait-on dans le CIIP Handbook après les attaques de ces derniers jours contre les gazoducs Nord Stream, les câbles de la Deutsche Bundesbahn ou encore le pont de Crimée? Au moins trois constats:

- La haute fragilité d'infrastructures linéaires pratiquement indéfendables sur des dizaines voir parfois des milliers de kilomètres et souvent même dans des endroits inaccessibles. Nous avons souvent évoqué dans nos billets la possibilité que les belligérants s'en prennent également aux câbles sous-marins qui transportent plus de 95% des données dans le monde. Le passage à l'acte semble être bien plus qu'une hypothèse de travail.
- La difficulté, dans le brouillard de la guerre pour désigner les coupables, la fameuse «attribution ». Nord Stream saboté par les Russes? Un non-sens pour certains analystes voyant la Russie privée d'un investissement de 20 mia $, d'une source majeure de revenus et d'un instrument idéal de chantage alors que le maniement du robinet aurait suffi.
- L'interdépendance totale entre des infrastructures vitales pour notre société toujours plus densément numérisée. Car ne nous y trompons pas, souvent les ponts ne servent pas qu'au passage de véhicules et de marchandises, mais aussi au transit de l'énergie et des données.

Nous ne pouvons que conseiller la relecture du rapport 2020 sur l'analyse nationale des risques et la stratégie nationale pour la protection des infrastructures critiques. À la lumière des trois événements mentionnés ci-dessus, il apparaît que la guerre ne se limite pas à l'est de l'Ukraine et au champ de bataille traditionnel. Notre civilisation fonctionne en multiples réseaux fragiles, une force indéniable en temps de paix, mais une vulnérabilité majeure quand la résilience n'est pas intégrée «by design». Une leçon que le monde numérique peine toujours à entendre.

Was würde nach den Angriffen der letzten Tage auf die Nord Stream-Pipeline, die Kabel der Deutschen Bundesbahn oder die Krim-Brücke in diesem CIIP Handbuch stehen? Mindestens drei Feststellungen:

- Die hohe Fragilität linearer Infrastrukturen, die über Dutzende, manchmal sogar Tausende von Kilometern und oft sogar an unzugänglichen Orten praktisch nicht verteidigt werden können. In früheren Beiträgen haben wir oft die Möglichkeit erwähnt, dass die Kriegstreiber auch die Unterseekabel angreifen könnten, die mehr als 95% der weltweiten Daten transportieren. Dabei handelt es sich scheinbar um mehr als eine Arbeitshypothese.
- Die Schwierigkeit, im Nebel des Krieges die Schuldigen zu benennen, die berühmte «Attribution». Nord Stream von den Russen sabotiert? Für gewisse Analysten ein Unsinn, da Russland einer Investition von 20 Mrd $, einer wichtigen Einnahmequelle und eines idealen Erpressungsinstruments beraubt wurde, während die Handhabung des Gashahns ausreichte.
- Die totale Interdependenz zwischen Infrastrukturen, die für unsere immer stärker digitalisierte Gesellschaft lebenswichtig sind. Denn machen wir uns nichts vor: Brücken dienen oft nicht nur der Überquerung von Fahrzeugen und Waren, sondern auch dem Transit von Energie und Daten.

Wir können nur empfehlen, den Bericht 2020 über die nationale Risikoanalyse und die nationale Strategie für den Schutz kritischer Infrastrukturen erneut zu lesen. Die drei oben genannten Ereignisse zeigen, dass der Krieg nicht auf den Osten der Ukraine und das traditionelle Schlachtfeld beschränkt ist. Unsere Zivilisation ist vielfältig vernetzt – eine unbestreitbare Stärke in Friedenszeiten, aber eine grosse Verwundbarkeit, wenn die Widerstandsfähigkeit nicht «by Design» eingebaut wird. Ein Fact, mit dem sich die digitale Welt noch immer schwertut.

Cyberactualité internationale

- **Hacking patriotique** – À l'heure où le monde occidental se ligue contre la Russie, il est naturel pour beaucoup de hackers de s'engager pour une cause évidente. Certes, mais avant de se lancer tête baissée, quid des conséquences? Car cela revient à remettre nous-mêmes en question les normes existantes sur la participation des civils à la guerre (et d'en faire des cibles légitimes), sur l' applicabilité des lois sur les conflits armés au cyberespace et la responsabilité des États pour les cyberdélits. En clair à bafouer nous-mêmes les normes dont nous reprochons – à juste titre – à la Russie leur violation.
- **Cyber in War** – La question cyber qui continue à animer les analystes est «s'est-on totalement trompé sur la nature de la partie cyber de la guerre?». Nous répétons depuis le début notre scepticisme face aux déclarations péremptoires et vous invitons à découvrir trois articles particulièrement éclairants (1, 2, 3) au sujet d'un conflit où les premières leçons ne peuvent en aucun cas être généralisées et où il ne faut pas oublier que pour détruire une infrastructure, une bombe reste un moyen infiniment plus rapide et meilleur marché. Cela étant, l'ENISA rappelle fort à propos que ce n'est pas fini.
- **Iran** – Le meurtre de Mahsa Amini par des policiers iraniens a déclenché une tempête et on mesure à quel point la maîtrise d'Internet est une arme massive en main de certains régimes pour faire taire la rue. Deux phrases illustrent combien l'information est importante. «Quand vous voyez d'autres personnes ressentir la même chose, vous devenez plus courageux» et «Quand Internet est coupé... tu te sens seul».
- **Daily business** – Les risques d'escalade du conflit à l'est de l'Europe sont vertigineux et le Président Biden parle même de risque

Internationale Cyberaktualität

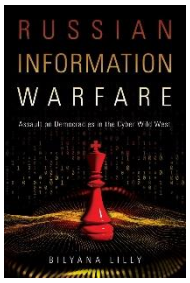
- **Patriotisches Hacking** - In einer Zeit, in der sich die westliche Welt gegen Russland verbündet, gehört es für viele Hacker zur Selbstverständlichkeit, sich für eine naheliegende Sache zu engagieren. Doch bevor man sich Hals über Kopf in die Sache stürzt, sollte man die Konsequenzen bedenken. Denn das bedeutet, dass wir selbst die bestehenden Normen zur Beteiligung von Zivilisten am Krieg (und sie zu legitimen Zielen zu machen), zur Anwendbarkeit der Gesetze über bewaffnete Konflikte im Cyberspace und zur Verantwortung von Staaten für Cyberverbrechen in Frage stellen. Im Klartext heisst das, dass wir die Normen, deren Verletzung wir – zu Recht – Russland vorwerfen, selbst missachten.
- **Cyber in War** - Die Cyberfrage, die die Analysten immer wieder umtreibt, lautet: «Haben wir die Natur des Cyberanteils des Krieges völlig falsch eingeschätzt?». Wir wiederholen von Anfang an unsere Skepsis gegenüber pauschalen Erklärungen und laden Sie ein, drei besonders aufschlussreiche Artikel (1, 2, 3) über einen Konflikt zu lesen, in dem die ersten Lehren keinesfalls verallgemeinert werden können und in dem man nicht vergessen darf, dass eine Bombe immer noch ein unendlich schnelleres und billigeres Mittel ist, um eine Infrastruktur zu zerstören. Die ENISA weist jedoch darauf hin, dass dies noch nicht das Ende der Fahnenstange ist.
- **Iran** – Der Ermordung von Mahsa Amini durch iranische Polizisten löste einen Sturm aus und zeigt, wie sehr die Kontrolle über das Internet eine massive Waffe in der Hand von bestimmten Regimen, um die Strasse zum Schweigen zu bringen. Zwei Sätze veranschaulichen, wie wichtig Informationen sind. «Wenn du siehst, dass es anderen genauso geht, wirst du mutiger» und «Wenn das Internet abgeschaltet ist ... fühlst du dich einsam».

d'Armageddon face à la tentation croissante des Russes, dos au mur, de faire usage d'armes nucléaires. Mais n'oublions pas le quotidien, car les dégâts infligés à la société par les cybercriminels restent obstinément astronomiques. Après un pic annoncé il y a un an de 223 Mia € pour 2020, le BITKOM a refait ses calculs et annonce 203 Mia € de pertes en 2021 pour l'économie allemande, soit 5.6% du PIB. Et 45% des entreprises allemandes pensent même que les cyberattaques peuvent menacer leur existence commerciale, alors que ce chiffre n'était que de 9% il y a un an.

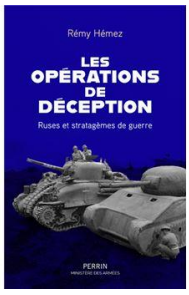
- **Daily business** – Die Risiken einer Eskalation des Konflikts im Osten Europas sind schwindelerregend und Präsident Biden spricht angesichts der wachsenden Versuchung der Russen, Atomwaffen einzusetzen, sogar von Armageddon. Aber vergessen wir nicht den Alltag, denn der Schaden, den Cyberkriminelle der Gesellschaft zufügen, ist nach wie vor astronomisch hoch. Nach einem Höchststand von 223 Mrd. € im Jahr 2020 hat der BITKOM erneut nachgerechnet und für 2021 Verluste von 203 Mrd. € für die deutsche Wirtschaft prognostiziert, was 5,6% des BIP entspricht. 45% der deutschen Unternehmen glauben sogar, dass Cyberangriffe ihre wirtschaftliche Existenz bedrohen könnten, während diese Zahl vor einem Jahr nur 9% betrug.

BOOKS

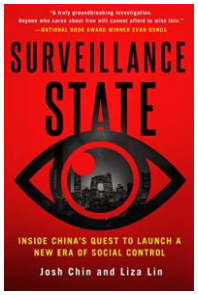
Russian Information Warfare



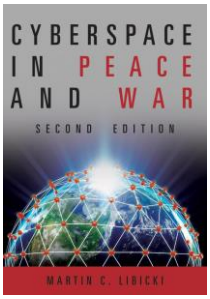
Les Opérations de déception



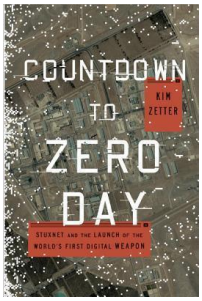
Surveillance State: Inside China's Quest to Launch a New Era of Social Control



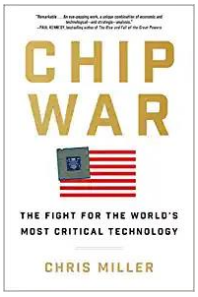
Cyberspace in Peace and War



Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon



Chip War: The Fight for the World's Most Critical Technology



Les faits marquants en Suisse durant la dernière quinzaine

- **Objectifs du Conseil fédéral** – Sur le plan numérique, 2023 s'avère d'ores et déjà passionnante avec de nombreux sujets et notamment: ▶ l'orientation à donner à l'Administration numérique suisse (ADS), ▶ la stratégie de l'administration fédérale en matière de transformation numérique et d'informatique pour les années 2024–2027, ▶ le message relatif à la nouvelle loi sur l'e-ID, ▶ le message relatif à une loi fédérale sur le système national de consultation des adresses des personnes physiques (loi sur le service des adresses), ▶ le message relatif au programme consacré à la transformation numérique dans le domaine de la santé ▶ la consultation relative à la révision de la loi fédérale sur le dossier électronique du patient, ▶ le message sur l'armée 2023 avec en particulier les investissements dans le domaine de la cyberdéfense, ▶la mise en vigueur de la loi sur la sécurité de l'information, ▶ la mise en œuvre des mesures prises en 2022 pour optimiser la protection des structures de la Confédération contre les cyberrisques, ▶ la consultation relative à l'ordonnance sur l'obligation qu'ont les exploitants d'infrastructures critiques de signaler les cyberattaques, ▶ la mise en vigueur de la loi sur la sécurité de l'information (LSI) et ses dispositions d'exécution. Et ce n'est pas dans la liste…, la création de l'office fédéral pour la cybersécurité qui devrait être opérationnel en 2024.

  Du numérique à toutes les sauces dira-t-on et la question clé est: «conduit par qui?». Car qui est le ministre du numérique, avec quels moyens, quelles compétences et quelles bases légales? **Il est en effet plus que l'heure de cesser de prendre le numérique pour une simple commodité et d'en faire un véritable domaine régalien**, comme la défense, les relations internationales, la santé, etc.

Die wichtigsten Ereignisse in der Schweiz während der letzten zwei Wochen

- **Ziele des Bundesrates** – Auf digitaler Ebene erweist sich das Jahr 2023 mit zahlreichen Themen bereits jetzt als spannend, untern anderem: ▶ die Ausrichtung der Digitalen Verwaltung Schweiz (DVS), ▶ die Strategie der Bundesverwaltung zur digitalen Transformation und Informatik für die Jahre 2024-2027, ▶ die Botschaft zum neuen e-ID-Gesetz, ▶ die Botschaft zu einem Bundesgesetz über das nationale Abrufverfahren für Adressen natürlicher Personen (Adressdienstgesetz), ▶ die Botschaft zum Programm zur digitalen Transformation im Gesundheitswesen, ▶ die Vernehmlassung zur Revision des Bundesgesetzes über das elektronische Patientendossier, ▶ die Botschaft zur Armee 2023, insbesondere die Investitionen im Bereich der Cyberdefence, ▶ die Inkraftsetzung des Informationssicherheitsgesetzes, ▶ die Umsetzung der 2022 getroffenen Massnahmen zur Optimierung des Schutzes der Bundesstrukturen vor Cyberrisiken, ▶ die Vernehmlassung zur Verordnung über die Meldepflicht von Cyberangriffen durch Betreiber kritischer Infrastrukturen, ▶ die Inkraftsetzung des Informationssicherheitsgesetzes (ISG) und seiner Ausführungsbestimmungen. Und auf der Liste fehlt noch … die Schaffung des Bundesamts für Cybersicherheit, das 2024 seine Arbeit aufnehmen soll.

  Digitales in allen Variationen, wird man sagen und die Schlüsselfrage lautet: «Von wem geführt?». Denn wer ist der Minister für Digitales, mit welchen Mitteln, welchen Kompetenzen und welchen Rechtsgrundlagen? **Es ist höchste Zeit, die digitale Welt nicht länger als Kommodität zu betrachten, sondern sie zu einem echten Regierungsbereich zu machen**, wie die Verteidigung, die internationalen Beziehungen, die Gesundheit etc.

- **La Poste fait l'acquisition d'Axsana** – Avec ce nouveau pas, la Poste prend une place clé dans le domaine du dossier électronique du patient. Avec les acquisitions précédentes (Tresorit, Hacknowledge), elle est désormais un acteur numérique majeur en Suisse.
- **Le contrôle fédéral des finances** rappelle l'administration fédérale à l'ordre – En effet, en matière de réaction aux cyberattaques, les départements sont trop lents à réagir et trop lents à annoncer au NCSC. À quoi bon avoir un bon capitaine avec Florian Schütz si le bateau prend l'eau?

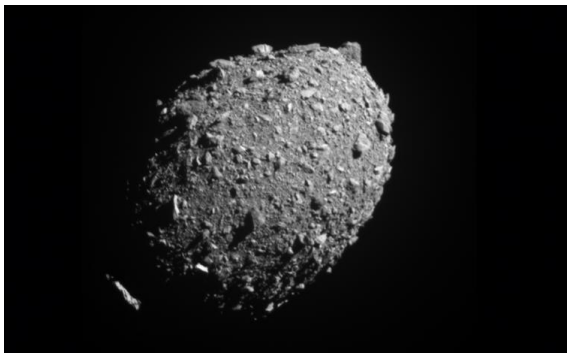
Et pour conclure…

… la rubrique fascination avec la Mission DART de la NASA (Double Asteroid Redirection Test) qui a réussi à entrer en collision avec l'astéroïde Dimorphos afin de changer sa trajectoire. Une belle victoire pour l'IT pour aussi ramener des images de cette qualité après 10 mois de voyage interplanétaire à 11 millions de km, près de 30 fois la distance Terre – Lune. Si les dinosaures avaient eu une telle technologie… !

- **Die Poste übernimmt Axsana** - Mit diesem Schritt übernimmt Die Post eine Schlüsselposition im Bereich des elektronischen Patientendossiers. Mit den vorherigen Übernahmen (Tresorit, Hacknowledge) ist sie nun ein wichtiger digitaler Akteur in der Schweiz.
- **Die Eidgenössische Finanzkontrolle** mahnt die Bundesverwaltung zur Ordnung – In der Tat reagieren die Departemente zu langsam auf Cyberattacken und melden sie zu langsam an das NCSC. Was nützt es, mit Florian Schütz einen guten Kapitän zu haben, wenn das Schiff leckschlägt?

Und zum Schluss …

… die Rubrik Faszination mit der DART-Mission der NASA (Double Asteroid Redirection Test), der es gelang, mit dem Asteroiden Dimorphos in Kollision zu treten, um seine Flugbahn zu ändern. Ein grosser Erfolg auch für die IT, nach 10 Monaten interplanetarer Reise in 11 Millionen km Entfernung – fast 30 Mal die Distanz Erde-Mond – Bilder dieser Qualität zu liefern. Hätten die Dinosaurier eine solche Technologie gehabt…!



Nous vous souhaitons une enrichissante découverte des articles et liens sélectionnés et nous réjouissons de vous retrouver dans 15 jours.

Wir wünschen Ihnen viel Spass beim Entdecken der ausgewählten Artikel und Links und freuen uns darauf, Sie in zwei Wochen 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.*