Les billets[i] de *digi*Volution / *digi*Volution's Newsletters
[21.06.2022 – 53ème édition]

Measure of success

Chers Lectrices et Lecteurs

Voici les ***d*V-News 13-2022** et leur sélection d'articles et de liens pour illustrer l'actualité de la dernière quinzaine. Par suite d'un nouvel article mettant en doute le cyber en tant qu'effecteur clé dans la guerre en Ukraine, nous avons consacré une part significative de cette édition à cette thématique. Cette manière de nier l'existence de cyberattaques de niveau systémique, uniquement parce que celles-ci n'auraient pas encore été observées dans cette guerre, est à notre sens un dangereux chemin; en effet, cela encourage la démobilisation face aux défis du cyber qui, d'un coup, … ne seraient pas si dangereux en temps de guerre.

Les métriques du *cyber in war*

Comment donc mesurer le succès des moyens cyber sur la base de l'exemple du conflit en cours en Ukraine? La question est éminemment difficile et nous nous garderons bien d'y apporter une réponse définitive. Nous y avons identifié trois facettes:

- **Entre réalité et perception** – Ce que nous voyons n'est qu'une fraction de la réalité; tirer des conclusions qui sont donc applicables pour l'avenir nous semble ainsi pour le moins léger. Le renseignement en source ouverte (surtout au travers des médias sociaux) ne montre de loin pas tout et il est susceptible aux manipulations par ajouts, soustractions, dissimulations, etc. ; de plus, il cible des publics dont l'esprit cri-

Liebe Leserinnen und Leser

Dies sind die ***d*V-News 13-2022** und unsere Auswahl von Artikeln und Links, die die Nachrichten der letzten zwei Wochen aufzeigen. Aufgrund eines neuen Artikels, der Cyber als Schlüsseleffekt im Krieg in der Ukraine in Frage stellt, haben wir einen bedeutenden Teil dieser Ausgabe diesem Thema gewidmet. Die Sichtweise, die Existenz von Cyberattacken auf systemischer Ebene zu bestreiten, nur weil sie in diesem Krieg noch wenig beobachtet wurden, ist unserer Meinung nach ein gefährlicher Weg, da er die Demobilisierung gegenüber den Cyberherausforderungen, die plötzlich … in Kriegszeiten nicht mehr so gefährlich wären.

Die Metriken des *Cyber in war*

Wie kann man den Erfolg von Cybermitteln am Beispiel des aktuellen Konflikts in der Ukraine messen? Dies ist eine äusserst schwierige Frage, und wir werden uns hüten, eine endgültige Antwort zu geben. Wir haben dort drei Facetten identifiziert:

- **Zwischen Realität und Wahrnehmung** – Was wir sehen, ist nur ein Bruchteil der Realität; daraus Schlussfolgerungen zu ziehen, die für die Zukunft gelten, erscheint uns somit zumindest leichtfertig. Open-Source-Informationen (vor allem über die sozialen Medien) zeigen bei weitem nicht alles. Sie sind anfällig für Manipulationen durch Hinzufügen, Weglassen, Verschweigen, usw. und richten sich an ein Publikum, dessen kritischer Geist bereits von den

tique est déjà rongé par les vagues d'émotions qui se sont emparées de l'Occident. Les guerres du Golf ont d'ailleurs été déclenchées grâce à de tels mécanismes. Dans les premiers jours de la guerre, alors que le rouble s'effondrait, certains experts prédisaient déjà la mort subite de l'économie russe; mais trois mois plus tard, la monnaie russe est à son niveau record de l'été 2015 et la Russie engrange des bénéfices sans précédents grâce au pétrole et au gaz. Un peu d'humilité chez les commentateurs ne feraient pas de mal.

- **Les objectifs réels des Russes** – À notre connaissance, aucun de ces experts qui peuplent les plateaux télé ne campe dans le bureau du président russe. Et si c'était le cas, quelle garantie aurions-nous qu'il rapporte la vérité? Si l'on ne connaît pas ces objectifs, ce qui remonte du terrain n'est que de l'information en sources ouvertes dont on ne peut pas tirer grand-chose ; ce ne sont pas des renseignements vérifiés le long d'un processus rigoureux. Comment savoir ainsi avec certitude quelles sont les avancées réelles des uns et des autres? Poutine voulait-il vraiment occuper tout le pays et s'emparer de Kiev? Avec un peu de recul et d'objectivité, il semble pourtant que certaines manœuvres des Russes aient d'abord eu pour objectif de fixer les forces ukrainiennes pour avoir les mains libres ailleurs. Quelle part de cyber les Russes ont ainsi mis dans leurs lignes d'opérations? Bien malin qui peut le dire.
- **L'absence de vue systémique et de temps long** – Une guerre comme celle qui frappe l'Ukraine et dont les conséquences vont lourdement impacter l'Europe dès cet automne, est par nature VUCA. Les succès tactiques engrangés ici ou là par les différentes parties belligérantes ne suffisent pas à décrire la situation réelle. Ceux qui ont bénéficié d'une formation militaire de haut niveau savent que l'analyse requiert au moins une approche de type PMESII-PT

Wellen der Emotionen, die den Westen erfasst haben, erschüttert ist. Die Golfkriege wurden durch solche Mechanismen ausgelöst. In den ersten Tagen des Krieges, als der Rubel zusammenbrach, sagten einige Experte bereits den Tod der russischen Wirtschaft voraus, aber drei Monate später ist die russische Währung wieder auf dem Recordstand vom Sommer 2015 und Russland erzielt beispiellose Gewinne aus dem Öl- und Gasgeschäft. Ein wenig Demut unter den Kommentatoren könnte nicht schaden.

- **Die realen Ziele der Russen** – Soweit wir wissen, campiert keiner der Experten, die in den Fernsehstudios sitzen, im Büro des russischen Präsidenten. Und wenn sie es täten, wie könnten wir dann sicher sein, dass sie die Wahrheit berichten? Wenn wir diese Ziele nicht kennen, sind die Informationen, die von der Basis kommen, nur Informationen aus verdeckten Quellen und keine Nachrichten, die in einem strengen Verfahren überprüft wurden. Wie soll man da wissen, welche Fortschritte, die eine oder andere Seite tatsächlich gemacht hat? Wollte Putin wirklich das ganze Land besetzen und Kiew erobern? Mit etwas Abstand und Objektivität scheint es jedoch, dass einige Manöver der Russen in erster Linie darauf abzielten, die ukrainischen Streitkräfte zu binden, um ihnen freie Hand zu lassen. Wie viel Cyber haben die Russen in ihre Operationslinien eingebaut? Ein Schelm, wer Böses dabei denkt.
- **Fehlende systemische- und Langzeitperspektive** – Ein Krieg wie derjenige in der Ukraine, dessen Folgen Europa ab diesem Herbst stark beeinflussen werden, ist von Natur aus VUCA. Die taktischen Erfolge, die die verschiedenen Kriegsparteien hier und da erzielt haben, reichen nicht aus, um die reale Situation zu beschreiben. Diejenigen, die eine solide militärische Ausbildung genossen haben, wissen, dass die Analyse zumindest einen PMESII-PT-Ansatz erfordert (politics, military, economy,

(*politics, military, economy, society, information structure, infrastructure, physical environment, time*). Et sur le plan temporel, souvenons-nous de la rapidité avec laquelle les forces américaines ont vaincu les talibans et les circonstances de leur piteux retrait 20 ans plus tard. Gagner sur le plan tactique est une chose, mais dans la durée et sur le plan stratégique la réalité est souvent toute autre.

La « cyberguerre » (terme depuis longtemps dépassé et mal traduit de l'anglais) n'a pas eu l'effet escompté? Nous le disons depuis le début de la guerre: gardons-nous des conclusions hâtives qui ne servent qu'à justifier de vieilles thèses. L'absence de cyberattaques destructrices est-elle due aux succès de la défense, à l'absence d'attaques, ou à d'autres causes? Tout soldat sait que le succès se construit par une combinaison d'effets dans l'ensemble des sphères d'opérations, terre, mer, air, espace, information, électromagnétique et… cyber.

Alors même si l'attaque ultime, le Cyberarmageddon, ne s'est pas encore manifestée, cela ne veut pas dire que rien ne se passe. Pendant que les experts se disputent mettons à profit chaque minute pour améliorer notre sécurité et notre résilience dont nous avons déjà si souvent constaté les déficiences.

Ce n'est qu'avec une approche holistique et systémique qu'il est possible de réduire significativement la probabilité d'occurrence et le coût des dommages des cyberattaques ou des pannes. Et dans le cas de Skyguide aussi – semble-t-il par suite de la défaillance d'un composant secondaire – il s'agit de rester humble. D'ailleurs, en première analyse, l'incident a été bien géré. Reste la phase des « leçons apprises ».

Autres événements remarquables : Palantir et Google – Avec leur partenariat, un géant de la donnée et du renseignement est né. Avec quelles conséquences réelles en dehors des promesses sur les prospectus de bien servir

society, information structure, infrastructure, physical environment, time). Und was die Zeit angeht, sollten wir uns daran erinnern, wie schnell die US-Streitkräfte die Taliban besiegt haben und unter welchen Umständen sie sich 20 Jahre später erbärmlich zurückgezogen haben. Auf der taktischen Ebene zu gewinnen ist eine Sache, aber auf der langfristigen und strategischen Ebene sieht die Realität oft ganz anders aus.

Der « Cyberkrieg » (ein längst überholter und schlecht übersetzter Begriff aus dem Englischen) hat nicht die erhoffte Wirkung erzielt? Wir sagen es seit Beginn des Krieges: wir sollten uns vor voreiligen Schlussfolgerungen hüten, die nur dazu dienen, alte Thesen zu rechtfertigen. Ist das Ausbleiben von zerstörerischen Cyberangriffen auf eine erfolgreiche Verteidigung, auf das Ausbleiben von Angriffen oder auf andere Ursachen zurückzuführen? Jeder Soldat weiss, dass der Erfolg durch eine Kombination von Effekten aus allen Operationssphären, Land, See, Luft, Weltraum, Information, Elektromagnetik und... Cyber, erzielt wird.

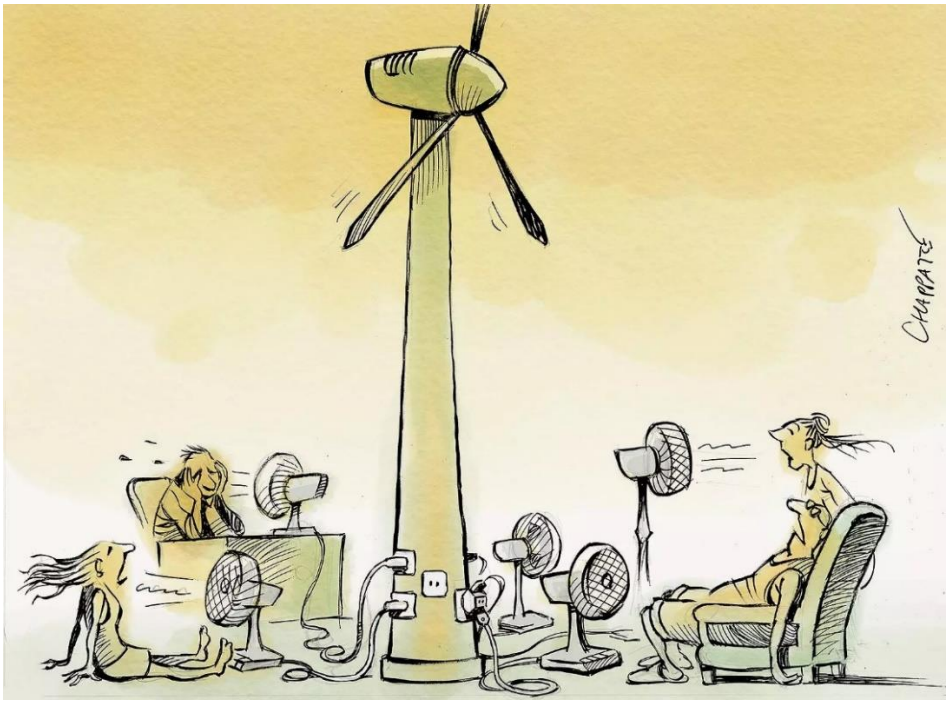
Selbst wenn der ultimative Angriff, das Cyberarmageddon, noch nicht stattgefunden hat, heisst das nicht, dass nichts passiert. Während sich also die Experten streiten, sollten wir jede Minute nutzen, um unsere Sicherheit und Resilienz zu verbessern, deren Schwächen wir bereits so oft festgestellt haben.

Nur mit einem ganzheitlichen und systemischen Ansatz können die Eintretenswahrscheinlichkeit eines Angriffs und die Kosten der dadurch entstehenden Schäden deutlich gesenkt werden. Auch im Fall von Skyguide – offenbar aufgrund des Versagens einer sekundären Komponente – gilt es, bescheiden zu bleiben. Auf den ersten Blick wurde der Vorfall gut gemeistert. Was nun bleibt ist die Phase der « Lessons Learned ».

Weitere bemerkenswerte Ereignisse: Palantir und Google – Durch diese Partnerschaft

leurs clients? Pour le comprendre, nous recommandons d'écouter la Prof. Ghernaouti. Sommes-nous en train d'atteindre les limites de notre société et de ses valeurs humanistes et démocratiques?

ist ein Daten- und Nachrichtendienstriese entstanden. Welche Konsequenzen hat dies, abgesehen von den Versprechungen in den Prospekten ihre Kunden gut zu bedienen? Um dies zu verstehen, empfehlen wir, Prof. Ghernaouti Gehör zu schenken. Sind wir dabei, an die Grenzen unserer Gesellschaft und ihrer humanistischen und demokratischen Werte zu stossen?



En Suisse durant les 15 derniers jours (à part la canicule)

L'obligation d'annoncer – C'est en 2017 qu'a été déposé un premier postulat réclamant l'obligation faite aux opérateurs d'infrastructures critiques d'annoncer les cyberattaques subies. La base légale n'est toujours pas en vigueur et le Conseil national vient d'approuver, de justesse, un nouveau postulat réclamant l'introduction d'une obligation de déclaration en cas de paiement de rançons et d'une obligation d'impliquer les autorités dans les négociations avec les criminels. À nouveau une bonne initiative, mais encore une demi-mesure, car limitée aux seuls ransomware. Et qui sera mise en place dans 5 ou 6 ans? Le temps de la politique n'est pas celui du cyber.

In der Schweiz während der letzten zwei Wochen (abgesehen von der Hitzewelle)

Meldepflicht – 2017 wurde ein erstes Postulat eingereicht, in dem gefordert wurde, dass die Betreiber kritischer Infrastrukturen verpflichtet werden sollten, erlittene Cyberangriffe zu melden. Die gesetzliche Grundlage ist noch immer nicht in Kraft und der Nationalrat hat gerade knapp ein neues Postulat angenommen, das die Einführung einer Meldepflicht für Lösegeldzahlungen und eine Verpflichtung zur Einbeziehung der Behörden in Verhandlungen mit Kriminellen fordert. Erneut eine gute Initiative, aber immer noch eine halbe Sache, da sie sich nur auf Ransomware beschränkt. Wird sie in fünf oder sechs Jahren umgesetzt? Die Zeit für Politik ist nicht die Zeit des Cyberaums.

Décollage des Women in cyber – Dommage que les dames soient obligées de créer une association pour enfin s'imposer dans les métiers du cyber, mais voici une initiative importante et à saluer, que *digi*Volution soutiendra avec conviction et enthousiasme. Une première manifestation de l'association se tiendra en septembre à Zurich.

Et à Berne nous avons relevé quatre développements significatifs.

- Une communication du NCSC sur les numéros de téléphone détournés et factures falsifiées.
- Le lancement des travaux pour des bases légales permettant la mise à disposition de géoregistres nationaux pour une Suisse numérique.
- Un rapport sur les rayonnements non ionisants qui montre que la population est exposée à des niveaux bien en dessous des valeurs limites; de bon augure pour rassurer les « anti-5G ».
- L'annonce d'une opération à laquelle ont participé nos autorités de poursuite pénale avec 11 autres pays pour démanteler l'organisation et l'infrastructure du logiciel malveillant FluBot qui s'attaquait aux téléphones Android.

Start der Women in Cyber – Eigentlich erstaunlich, dass die Damenwelt gezwungen ist, einen Verein zu gründen, um sich endlich im Bereich Cyber durchzusetzen, aber dies ist eine wichtige und begrüssenswerte Initiative, die *digi*Volution mit Überzeugung und Enthusiasmus unterstützen wird. Eine erste Veranstaltung des Vereins wird im September in Zürich stattfinden.

Und in Bern haben wir vier bedeutende Entwicklungen festgestellt.

- Eine Mitteilung des NCSC zu umgeleiteten Telefonnummern und gefälschten Rechnungen.
- Die Arbeiten an den gesetzlichen Grundlagen für die Bereitstellung von nationalen Georegistern für eine digitale Schweiz.
- Ein Bericht über nichtionisierende Strahlung, der zeigt, dass die Bevölkerung weit unterhalb der Grenzwerte exponiert ist; ein gutes Mittel, um die « Anti-5G-Bewegung» zu beruhigen.
- Die Ankündigung einer Operation, an der unsere Strafverfolgungsbehörden zusammen mit 11 anderen Ländern teilnahmen, um die Organisation und Infrastruktur der bösartigen Software FluBot zu zerschlagen, die Android-Telefone angriff.

Chez *digi*Volution

À Lille du 7 au 9 juin nous avons apporté notre soutien à notre ambassade de Paris qui avait mis en place avec le Swiss Business Hub un très beau pavillon au FIC (Forum International de la Cybersécurité). Et les Suisses se sont fait remarquer, notamment avec Marley, la mascotte de UBCOM.

Bei *digi*Volution

Wir waren in Lille vom 7. bis 9. Juni zur Unterstützung unserer Botschaft in Paris, die zusammen mit dem Swiss Business Hub einen sehr schönen Pavillon auf dem FIC (Internationales Forum für Cybersicherheit) aufgestellt hatte. Und die Schweizer machten sich bemerkbar, insbesondere mit Marley, dem Maskottchen von UBCOM.

Le 14 juin à Bucarest, à la Casa Elvetiei, nous avons été invités au Cyber Espionage Awareness Day for Business et à cette occasion avons publié une réflexion dans le journal Cybersecurity Trends.

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

Am 14 Juni in Bukarest, im Casa Elvetiei, waren wir beim Cyberspionage Awareness Day for Business eingeladen und konnten in der Zeitschrift «Cybersecurity Trends» einen Beitrag verfassen.

Wir wünschen Ihnen viel Spass beim Entdecken der ausgewählten Artikeln 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 https://www.digivolution.swiss/dv-blog/. Interessierte finden auf dieser Seite auch den Link zur Anmeldung.*