Kommentare zum sicherheitspolitischen Bericht 2021 des Bundesrates

digiVolution
prepare for the next

Kurz gefasst

Der Bericht des Bundesrates über die Sicherheitspolitik (SIPOL B) vom 14. April 2021 stellt eine deutliche Verbesserung[1] gegenüber früheren Ausgaben dar und ist zu begrüssen. Wir von *digi*Volution sind jedoch der Meinung, dass **dieses für unser Land so wichtige Dokument noch weiter gehen kann und muss.** Wir haben es analysiert – unter dem Gesichtspunkt der digitalen Mutation – und schlagen neue Massnahmen und Ansätze vor, die wir für zwingend erforderlich halten.

Zusammengefasst sind dies:

- Der SIPOL B soll eine echte Strategie mit Massnahmen werden, die für alle Beteiligten **verbindlich** sind; unsere Sicherheit darf nicht der Einfachheit, dem Komfort und den Sonderinteressen untergeordnet werden.
- **Alle Herausforderungen** berücksichtigen, die sich zu Gefahren oder Bedrohungen entwickeln können (holistischer Ansatz) und Entwicklung komplexer Denkfähigkeiten und -kapazitäten, um die stattfindenden Veränderungen, einschliesslich der übergreifenden digitalen Mutation, zu erkennen und zu verstehen (systemischer Ansatz).
- **Tief greifende Strategien** festlegen (vom Staat bis hin zum Individuum), insbesondere für die Cybersicherheit und den Schutz vitaler[2] Infrastrukturen; dazu gehört der Erlass von Standards und Anreizen für die Betreiber, die den Risiken für die Gesellschaft im Falle der Nichteinhaltung angemessen sind, sowie erhebliche Investitionen in die Sicherheit der Infrastruktur und in die Ausbildung.
- Die **Wahrung der digitalen Souveränität** zu den staatlichen strategischen Zielen hinzufügen und dort, wo es nötig und möglich ist (praktisch und finanziell), die geeigneten Massnahmen ergreifen, um gleichzeitig die Schweiz zu einem akademischen und industriellen Champion des digitalen Zeitalters zu machen.
- Wiedereinführung des **Vorsorgeprinzips**, Förderung einer **Kultur der Antizipation** und Schaffung einer Haltung der "**ständigen und differenzierten Bereitschaft**" (nach Sektoren), die die Schweiz aus ihrem abwartenden und reaktiven Modus herausführt.
- Die **strategischen und lebenswichtigen Interessen der Schweiz** klar definieren, was innerhalb eines bestimmten Zeitrahmens erreicht oder geschützt werden muss (inkl. der Mittel zur kontinuierlichen Messung ihres Erreichungsgrades).

[1] Mit Ausnahme der nur mittelmässigen redaktionellen Qualität der französischen Übersetzung.

[2] Zwingender Begriff, weil er "lebensbedrohlich" bedeutet und daher präziser und ausschliesslicher ist als der Begriff "kritisch", der ohne Qualifizierung alles und nichts aussagt.

Index

Gesamtbeurteilung

Die Stiftung *digi*Volution ist dankbar für die Möglichkeit, zum Entwurf des Sicherheitspolitischen Berichts des Bundesrates (SIPOL B) Stellung zu nehmen. Insgesamt sind wir der Meinung, dass **dieses Dokument eine deutliche Verbesserung gegenüber früheren Ausgaben darstellt**, insbesondere was die Massnahmen zur Bewältigung von Bedrohungen und Gefahren angeht. Wir sind jedoch der Meinung, dass **der Bericht ergänzt und weiterentwickelt werden muss, um dem systemischen Einfluss der digitalen Mutation besser Rechnung zu tragen**.

Wir haben **sechs Empfehlungsbereiche** formuliert, die wir für zwingend erforderlich halten, um zu verhindern, dass die Kluft zwischen "IST" und "SOLL" unumkehrbar wird. **Diese Empfehlungen sind jedoch keineswegs ein Aufruf zu "weniger konventionellem Militär", noch sind sie ein Aufruf zum Wettbewerb zwischen den Sicherheitsbereichen**. Die Experten von *digi*Volution sind sich der Art der Bedrohungen, denen die Schweiz ausgesetzt ist, wohl bewusst und sie sind sich auch bewusst, dass die Zeit, die benötigt wird, um die notwendigen Ressourcen bereitzustellen, die Zeit, die für die Entwicklung der Risiken benötigt wird, bei weitem übersteigt. Und es gibt allen Grund zu der Annahme, dass in naher Zukunft ein schwerer Konflikt ausbrechen könnte. **Es geht also nicht nur darum, "es besser zu machen", sondern vor allem darum, "mehr zu machen"**.

❶ Damit der Bericht zu einer Strategie wird

Was den Inhalt betrifft, so sind wir uns bewusst, dass **dieser Bericht kein "Weissbuch" ist** und einen Konsens zwischen vielen Akteuren mit vielfältigen und oft widersprüchlichen Interessen darstellt. **In dieser unverbindlichen Form liegt jedoch sein Hauptmangel**. Eine Seitenbegrenzung für ein so wichtiges Dokument für die Zukunft des Landes (wie uns berichtet wurde) dient nur dazu, seinen Inhalt unnötig zu verallgemeinern; in Zukunft muss diese Art von redaktioneller Zielsetzung abgeschafft werden, da sie keinerlei Einschränkung für das Konzept der Sicherheit der Schweiz darstellen darf. Im Gegenteil, **die anhaltende Verschlechterung der geopolitischen Lage macht es erforderlich, dass sich die Schweiz hinter ein umfassendes, starkes und kohärentes Projekt stellt**, bei dem die Massnahmen nicht systematisch in kleine, über viele Jahre verteilte Tranchen aufgeteilt werden, wie es heute meist der Fall ist.

Unsere Vorschläge – Dieser Bericht, der den Eckpfeiler der schweizerischen Sicherheitspolitik darstellt, **soll zu einer echten Strategie werden**, um eine starke Verbindung zwischen den verschiedenen Instrumenten, ihren Mitteln und ihrem Einsatz herzustellen. Eine solche Strategie soll konkrete Richtungen, Projekte und Mittel festlegen und als **verbindliche Referenz für alle beteiligten Akteure dienen**. Wir schlagen vor, **die Struktur der für die Gestaltung und Lenkung der Sicherheitspolitik zuständigen Gremien zu überprüfen und sie zu einem ständigen Kompetenzzentrum zu machen**, das nicht nur ein Büro für die periodische Koordinierung des SIPOL B und die Verwaltung der tagespolitischen Angelegenheiten dient. Vor dem Hintergrund der sich wandelnden Herausforderungen ist auch **eine Überprüfung des Begriffs der Neutralität und seiner Anwendbarkeit erforderlich, insbesondere im Hinblick auf die digitale Mutation**.

❷ Für einen ganzheitlichen und systemischen Ansatz

Die Analyse des Entwurfs des SIPOL B zeigt, dass bei seiner Entwicklung ein klassischer sektoraler (Silo-)Ansatz vorherrschte. Die steigenden Komplexität und Dynamisierung der Welt zeigen jedoch, dass eine solche Denkstruktur nicht mehr angemessen ist. Auch die Berichte früherer Jahrzehnte können nicht als Beispiel herangezogen werden, nach dem Motto "das haben wir schon immer so gemacht". Das Akronym VUCA[3] ist heute Realität. Die Suche nach dem Vorkommen der Begriffe, aus denen es sich zusammensetzt (auf Deutsch volatil, unsicher, komplex, mehrdeutig), oder die Analyse ihrer Folgen zeigt jedoch, dass sie nicht vorhanden sind. **Dieser Bericht gibt der Schweiz nicht die nötigen Impulse für ihre Sicherheit und Verteidigung der Zukunft**.

Viele Begriffe werden zwar erwähnt, aber nicht vertieft, und der Text enthält manchmal Aussagen, die wir für falsch halten. Dies gilt insbesondere für die technologischen Auseinandersetzungen zwischen den Chinesen und dem Westen, die keineswegs als "Zankerei" bezeichnet werden können, sondern im Gegenteil ein Wettrennen um die Vorherrschaft darstellen, ein Kampf, dessen Ausgang das strategische Gleichgewicht von morgen bestimmen wird.

Unsere Vorschläge – Der SIPOL B soll **alle Faktoren berücksichtigen, die die Sicherheit der Schweiz stärken oder schwächen**. Bereiche wie Urbanisierung, Rohstoffe, Energie, Wasser, Demografie, Einwanderung, Kultur und soziales Verhalten, Einfluss, Bildung und Forschung und natürlich der Klimawandel sollten nicht nur genannt, sondern rigoros und systemisch analysiert werden. Auf strategischer Ebene muss die Schweiz ihre **Kompetenzen und Fähigkeiten im Bereich des komplexen Denkens ausbauen und dabei auch die ganze Bandbreite der Mutationen erkennen und verstehen.**

❸ Für eine umfassende Cybersicherheit

Der digitale Raum stellt einen Paradigmenwechsel dar. Drei Qualifikationen beschreiben die Position der Schweiz und aller Staaten.

- Sie sind **abhängig** von privaten und öffentlichen systemischen Akteuren, die ihre Souveränität, d.h. ihre Fähigkeit, frei und autonom zu denken, zu entscheiden und zu handeln, missachten und bedrohen;
- Sie werden durch eine Vielzahl von Verletzlichkeiten **geschwächt**: technologische (z.B. Produkte, die fast unkontrolliert auf den Markt kommen, wie die vernetzte Objekte), logistische (z.B. die Versorgung mit wichtigen Ressourcen und Bauteilen) und menschliche (z.B. Mangel an qualifiziertem Personal oder die Kluft zwischen den Generationen);
- Sie werden von einer wachsenden Zahl böswilliger Akteure **bedroht**, die die Möglichkeiten des digitalen Raums für geopolitische, kriminelle, manipulative / desinformierende oder überwachende Zwecke missbrauchen; Der Wettlauf um Cyberwaffen wird zum Vorteil der Angreifer, die nicht zögern, die lebenswichtigsten

[3] Volatility, uncertainty, complexity and ambiguity.

Interessen und Dienste (private und öffentliche, einschliesslich Spitäler) anzugreifen, und denen der unzureichende politische, rechtliche und ethische Rahmen keinen Einhalt gebietet; so übersteigt der geschätzte Schaden (der rasch ansteigt) bereits über 1% unseres BIP, noch bevor es zu einem offenen Konflikt im digitalen Raum kommt; eine jüngste deutsche Studie spricht sogar von wirtschaftlichen Verlusten von über 6,6% des BIP.

Die Cybersicherheit entwickelt sich rasch weiter. Ursprünglich eine vertikale Aufgabe von Cyberverteidigern, die gegen Cyberangreifer vorgehen, ist es heute ein **bereichsübergreifendes und hochdynamisches Phänomen**, dem ein traditioneller Top-Down- und Silo-Ansatz nicht mehr gerecht wird. Die Bemühungen des Bundes in den letzten Jahren sind zu begrüssen, aber die Reaktionen sind zu langsam und ihr Umfang entspricht immer weniger den **Herausforderungen einer inzwischen systemischen Dimension**. **Die Kluft zwischen dem "IST" und dem "SOLL" vergrössert sich alarmierend.**

Der SIPOL B (Kapitel 4.2.5: Verstärkung des Schutzes vor Cyberbedrohungen) listet fast nur Massnahmen auf Bundesebene auf und ist vage formuliert mit "*Zur weiteren Verstärkung des Schutzes vor Cyberbedrohungen dienen insbesondere…*". Die International Telecommunication Union ITU stuft die Schweiz in Bezug auf die Maturität vor Cyberrisiken weltweit auf Platz 42 ein, und die Meldepflicht für Betreiber vitaler Infrastrukturen (BVI) ist seit 2017 im Parlament hängig. Noch gravierender ist, dass die seit langem bekannten Ergebnisse für die Stromversorgung (Bericht des BFE runterladen), unsere unmittelbar lebenswichtige Infrastruktur, nun öffentlich sind; dieser Bereich erreicht auf einer Skala von 0 bis 4 nicht einmal die Note 1! **Vertrauen und Eigenkontrolle sind an ihre Grenzen gestossen.** Im Gesundheitswesen oder im Strassenverkehr ist jeder verantwortlich und dafür sensibilisiert. Auf die Strasse wird sogar ein Führerschein verlangt, während Nachlässigkeit oder unangemessenes Verhalten mit zum Teil empfindlichen Strafen geahndet wird. Aber nichts von alledem im digitalen Raum, trotz der potenziell schwerwiegenden Folgen!

Unsere Vorschläge – Der Anwendungsbereich der Cybersicherheit sollte nicht länger auf den Staat und die BVIs beschränkt sein. Es müssen eine "**Cybersicherheit in der Tiefe**" und **klare Verantwortungsprinzipien** eingeführt werden, und zwar bis auf die Ebene des Individuums. Wie beim Schutz des Luftraums muss der **Grundsatz der Wahrung der digitalen Souveränität** erklärt und in Bereichen angewandt und umgesetzt werden, in denen dies notwendig und möglich ist, und zwar mit ausreichenden Mitteln. **BVIs müssen klare Cybersicherheitsstandards auferlegt werden**, die überwacht und gegebenenfalls **bei Verstössen gegen die Normen entsprechend den lebenswichtigen Risiken, die sie für die Gesellschaft verursachen, sanktioniert werden**.

❹ Für eine Politik der Antizipation und Vorsorge

Die Geschichte zeigt, dass die Schweiz seit dem Deutsch-Französischen Krieg von 1870-1871 systematisch von Konflikten überrascht wurde. Kürzlich wurde unser Land trotz mehrerer Warnungen erneut überrumpelt. Diesmal war es die Pandemie, bei der ein aktueller Bericht des BWL zeigt, dass die wirtschaftliche Versorgung des Landes zahlreiche Rückschläge erlitten hat. Massnahmen, die auf der Grundlage der Erkenntnisse aus der Sicherheitsverbundsübung 2014 (SVU 14) angeordnet wurden, sind nicht umgesetzt worden. Man kann sich zu Recht fragen, was der Zweck des Krisenfrüherkennungsorgan der

Bundeskanzlei ist, warum die Pandemie und das Risiko eines bewaffneten Konflikts im Bericht "Perspektiven 2030" von 2014 praktisch nicht vorkommen und warum dieser Bericht noch nicht aktualisiert wurde.

Die Liste der "Pannen" im Bereich der Antizipation ist lang. Die wenigen Arbeiten, die durchgeführt wurden, werden nicht systematisch weiterverfolgt. Begriffe wie "Business continuity", "Sorgfaltspflicht" oder "Vorausplanung" werden zwar häufig verwendet, indessen seltener angewendet. Die Schweiz investiert ungenügend in Antizipation und das Vorsorgeprinzip. Der Begriff "Sicherheit der Lieferkette" ist auf Messen in aller Munde, aber was wird getan, um zu verhindern, dass wir Opfer von Cyberangriffen werden, wie sie kürzlich insb. die USA heimgesucht haben? Auf allen Ebenen und in allen Organisationen – neuerdings sogar beim NCSC – ist zu beobachten, dass die dringend erforderliche Aufstockung der personellen und finanziellen Mittel für die Cybersicherheit zurückgehalten wird, was im Widerspruch zu dem steht, was gesagt wird und zu den Herausforderungen. Es ist auch bekannt, dass bis 2026 rund 20% der IKT-Fachkräfte fehlen werden. Die Unternehmen werden dann keine andere Wahl haben, als die Qualität ihrer Dienstleistungen zu verringern, auf Innovationen zu verzichten, Aufgaben ins Ausland zu delegieren oder Allianzen zu bilden, die die Abhängigkeiten, die Risiken der Spionage oder die Übernahme durch Konkurrenten vervielfachen werden.

Der Bereich Bildung, Forschung und Innovation (BFI) wird im SIPOL B kaum erwähnt. Der Begriff "Ausbildung" kommt nicht vor; der Begriff "Forschung" erscheint 3 Mal und "Innovation" nur einmal. Sicherheit (Cyber oder generell) lässt sich nicht verordnen und kann nicht ab Lager gekauft werden. Ohne bedeutende Investitionen in den oben genannten Bereichen wird die Schweiz nur ein Technologiekonsument mit immer grösserer Abhängigkeit sein und damit an Souveränität einbüssen.

Unsere Vorschläge – Wir müssen **die Erfahrung und diejenigen, die sie haben, aufwerten** (was wäre, wenn wir die Fähigkeiten der Senioren nutzen würden?), ein **starkes Vorsorgeprinzip wiederherstellen** und eine **Kultur der Antizipation fördern**, damit wir in Sachen Sicherheit unsere reaktive Haltung durch eine proaktive ersetzen. Dann müssen wir auf der aussergewöhnlichen Basis, die wir (noch) haben, die **Schweiz zu einem akademischen und industriellen Champion der digitalen Technologie** für sich selbst und für die Eroberung von Märkten machen, nach dem Beispiel von Israel und Estland. Schliesslich muss diesen Entwicklungen eine **globale Bestandsaufnahme und eine Bewertung der existierenden Antizipations- und Präventionsmassnahmen** vorausgehen.

❺ Für ein Verteidigungskontinuum

Beim Zerfall der Berliner Mauer, feierte die westliche Welt den Triumph ihrer Ideen und das Fehlen von Alternativen zu ihrer liberalen Doktrin. Einige Intellektuelle sprachen sogar vom "Ende der Geschichte". Als der sowjetische Feind in die Knie ging, wich die Angst vor einem Weltkrieg der Illusion einer Friedensdividende. Die Schweiz hat daraufhin ihre Budgets gekürzt und sogar deren *Halbierung* riskiert, bevor sie sich einbildete, ihren militärischen Rückstand im Krisenfall durch eine Doktrin des "*Aufwuchs-Konzept*" aufholen zu können. Im Jahr 2009 wurde der Bundesrat vom Parlament aufgefordert, sich mit den potenziellen Konflikten infolge der Wirtschaftskrise zu befassen. Er antwortete: "*Sollte ein Aufwuchs der Armee einmal erforderlich sein, so wird die Art der konkret sich abzeichnenden Bedrohung*

entscheidend sein für Art, Umfang, Kosten und Dauer der zu treffenden Aufwuchsmassnahmen."

Die Sicherheitsdoktrin der Schweiz ist somit in erster Linie reaktiv, weitgehend militärisch, symmetrisch und vor allem durch die Budgets bestimmt. Was ist mit der "*konkret sich abzeichnenden Bedrohung* " in der oben erwähnten Antwort gemeint? Wie ist die aktuelle Situation in der Schweiz und in welchem Bereich? Wie viel Zeit muss sie haben, um eine Krise zu bewältigen? In der Schweiz wird die Sicherheitslage traditionell in drei Kategorien eingeteilt: "normal", "besonders" und "ausserordentlich". Diese Einteilung findet sich zum Beispiel in den "*Weisungen über organisatorische Massnahmen in der Bundesverwaltung zur Bewältigung besonderer und ausserordentlicher Lagen*", im Gesetz über den Wetterdienst, im Pandemiegesetz oder im Armeegesetz. Wir sind der Meinung, dass diese Kategorisierung zu einer starken kognitiven Verzerrung führt, die der rechtzeitigen Bereitstellung angemessener Ressourcen abträglich ist.

Wie viel Zeit bliebe uns im Falle eines massiven Cyberangriffs zwischen der normalen und der besonderen und ausserordentlichen Lage? Finden wir auf dem Markt die Ausrüstung und das Personal, um die Lücken in unseren Systemen rechtzeitig zu schliessen?

Seit Anfang der 2000er Jahre gibt es viele Anzeichen dafür, dass sich die Konfliktsituation verändert. Zwei chinesische Offiziere formulierten dies bereits 1999 in ihrem Buch "Unrestricted Warfare". Dieser wichtige Beitrag ist im Westen leider weitgehend unbekannt geblieben. Er beschreibt eine Doktrin unterhalb der Kriegsschwelle, die alle Bereiche der Gesellschaft angreift, um den Gegner strategisch zu besiegen und eine dauerhafte Vorherrschaft zu errichten. Diese Prinzipien werden bereits von einigen Staaten (allen voran China[4] und Russland) angewandt und gehen weit über konventionelle militärische Visionen hinaus, bei denen die **Vervielfältigungs-, Verstärkungs- und Beschleunigungseffekte des und durch den digitalen Raum nicht verstanden werden**.

Die rasche und tiefgreifende Veränderung unserer cyber-bio-physikalischen Gesellschaft, die durch den ausserordentlichen technologischen Fortschritt der letzten 20 Jahre vorangetrieben wurde, hat das Feld der Möglichkeiten beträchtlich erweitert, und wir befinden uns heute in einem Zustand des permanenten Konflikts, der von denjenigen, die die reale Situation relativieren, prosaisch, ja naiv als "Wettbewerb" bezeichnet wird. In der unmittelbaren Zukunft spielt sich für die Schweiz alles unterhalb der Kriegsschwelle ab, meist ausserhalb des militärischen Bereichs und auch in einem immateriellen Rahmen. Diese Angriffe sind schwer zu erkennen und scheinen harmlos zu sein, weil sie sich in einer gewissen Normalität verstecken. Es handelt sich jedoch um eine echte Form des Konflikts.

Unsere Vorschläge – Verzicht auf den modischen Begriff des "hybriden Konflikts" (amerikanischer Herkunft, und weder in unserer Doktrin definiert noch in unseren materiellen Mitteln umgesetzt), der keinen Mehrwert bringt; die Untersuchung von Konflikten zeigt, dass alle dieses Merkmal aufweisen und dass die konfliktführenden Parteien bereits alle vorhandenen Mittel und Waffen einsetzen, um ihre Ziele zu erreichen. **Verzicht auf die Klassifizierung in *normal*, *besonders* und *ausserordentlich*** und **Schaffung einer Kultur und einer Haltung der "ständigen und differenzierten Bereitschaft"** nach Sektoren, welche die Schweiz aus dem abwartenden und reaktiven Modus herausführt, der

[4] China ist ein strategischer Konkurrent, der die **universellen Werte**, die sich die Nationen nach dem Zweiten Weltkrieg gesetzt haben, nicht teilt. Diese grosse Gefahr wird im SIPOL B nicht behandelt.

gleichbedeutend ist mit Überraschung und somit mit Niederlage. Umsetzung einer **"Verteidigung in der Tiefe" des Landes und seiner vitalen Infrastrukturen** (Antizipation - Erkennung - Schutz - Anpassung - Widerstandsfähigkeit - Verteidigung - Wiederherstellung des Normalzustands – kontinuierlichen Verbesserung), wobei die **digitalen Aspekte übergreifend integriert** werden.

❻ Für den Schutz vitaler Infrastrukturen

Es ist noch gar nicht so lange her, dass die breite Öffentlichkeit Computer als etwas Optionales betrachtete, als eine "zusätzliche Spielerei", eine "verbesserte Schreibmaschine", "nur für Freaks". Viele betrachteten "Star Trek", "2001: Odyssee im Weltraum", "Terminator" oder "Minority Report" als unrealistische Vorstellungen oder Dystopien. "Das wird nie passieren!". In der Zwischenzeit gehören viele der in diesen Fiktionen auftauchenden Technologien zu unserem Alltag, und viele der von Branchenvisionären wie Ray Kurzweil oder Bill Gates angekündigten Entwicklungen werden auch Wirklichkeit. Der digitale Raum steht heute im Zentrum der Gesellschaft. Wir haben es mit einer **Mutation** zu tun, d. h. mit einer Situation, **von der wir unweigerlich und unumkehrbar abhängig sind und deren Scheitern zum Zusammenbruch der Gesellschaft führen würde**.

Ohne IKT und Strom wären viele lebenswichtige Dienstleistungen (Gesundheit, Energie, Finanzen, Verkehr, Wasser, Lebensmittel usw.) sofort nicht mehr verfügbar. Unsere Gesellschaft ist so komplex und ihre Abhängigkeiten so zahlreich, dass wir nicht wissen, wie oder wie lange es dauern würde, den "Motor wieder anzuschalten". Nach einigen Tagen der Nichtverfügbarkeit würde der Schaden für das Leben und das Wirtschaftsgefüge schwerwiegend, dann dramatisch und nach einigen Wochen wahrscheinlich irreversibel werden. Was ist mit den Plünderungen und der Gewalt, die dies verursachen wird? Die Bilder aus den Läden während dem Teil-Lockout im Jahr 2020 sind nur ein Vorgeschmack auf die Panik – verstärkt durch die sozialen Medien solange diese funktionieren – und ihre Folgen, die explodieren könnten. Doch für die Schweiz ging es im Jahr 2020 noch nicht um eine Lebenbedrohung. Die Abschaltung von lebenswichtigen Infrastrukturen und Diensten hätte aber eine ganz andere Bedeutung. Und man bräuchte keine "Boots on the ground" von einem Luft-Boden-Feind, um sie lahm zu legen; aber er wird später kommen. Es ist daher zwingend notwendig, entschlossen zu handeln, bevor der Schaden nicht mehr tragbar ist.

Unsere Vorschläge – Zusätzlich zu den in Punkt 3 vorgeschlagenen Massnahmen (Auferlegung eines klaren Cybersicherheitsstandards für BVIs, dessen Überwachung und Sanktionierung von Verstössen entsprechend den lebenswichtigen Risiken, die sie für die Gesellschaft darstellen) ist eine **Neubewertung der Mittel und Rollen des Staates und der BVIs beim Schutz der letzteren erforderlich**, die in Bezug auf Kompetenzen und Mittel inzwischen weitgehend überfordert sind. **Um die Sicherheit und Souveränität der Schweiz zu gewährleisten, müssen wichtige staatliche Investitionen getätigt werden**.

Konklusion

Der SIPOL B 2021 ist ein deutlicher Fortschritt gegenüber früheren Fassungen. Allerdings weist er erhebliche Mängel auf und **sein Charakter als "Bericht" erlaubt es nicht, konkrete Massnahmen aufzuerlegen**.

In Bezug auf Ziffer 3.3, die Ziele "[...] *ergeben sich folgende spezifischen Ziele als Schwerpunkte der Sicherheitspolitik in den kommenden Jahren*", werden weder ein Anspruchsniveau noch einen Zeitrahmen für ihre Erreichung bestimmt. Dies Ziele definieren und verteilen nicht die zur ihrer Erreichung notwendigen Rollen. Alles in allem ist es ein "Tiger ohne Zähne".

Insgesamt zeigt dieser Bericht ein **mangelndes Verständnis für die Folgen der digitalen Mutation und seine transversalen und systemischen Auswirkungen auf alle Bereiche der Gesellschaft**. Der Bericht beschränkt sich auf den regalistischen Ansatz der Sicherheitspolitik, "top-down" mit seinen historischen Akteuren, und **verkennt die Notwendigkeit, die Sicherheit der Schweiz in der Tiefe zu verankern**. Bestimmte Begriffe, die durch ein geringes Vorkommen von Schlüsselbegriffen (insbesondere im Bereich BFI – Bildung, Forschung. Innovation) hervorgehoben werden, zeigen einen **konzeptionellen Mangel unserer Sicherheitspolitik** auf.

Frühwarnung ist ein wichtiges Ziel, aber wenn man Ziel 7 "*Stärkung der Widerstandsfähigkeit und Versorgungssicherheit bei internationalen Krisen*" liest, kann man sich des Eindrucks nicht erwehren, dass **Antizipation nicht verstanden wird**. **Massnahmen, die "für den Krisenfall" ergriffen werden, kommen immer zu spät**. Mit der Hyperkonnektivität und den sich daraus ergebenden Abhängigkeiten besteht auch die grosse Gefahr, dass Krisen zunehmend zu "Multikrisen" (multidimensional) werden. Sind die Führungsstrukturen darauf abgestimmt? Was haben wir von COVID gelernt?

Es wird sicherlich nicht möglich sein, alle Überraschungen zu vermeiden, da die allgemeine Hektik, in der wir erleben, die Wahrscheinlichkeit ihres Auftretens nur noch erhöht. Aber es ist nicht länger hinnehmbar, dass wir, wie im Fall von COVID, in Bereichen überrascht werden, die zwar identifiziert wurden, für die Massnahmen angeordnet wurden, die aber nicht umgesetzt und nicht überwacht werden.

Das Wort "Zukunft" kommt in dem Dokument nur dreimal vor. Dies entspricht dem Bericht-Titel des SIPOL B, zeigt aber wie es zwingend notwendig wäre, **diesem Dokument eine Zukunftsorientierung zu geben** und dafür zu wissen, **was die vitalen Interessen der Schweiz sind**.

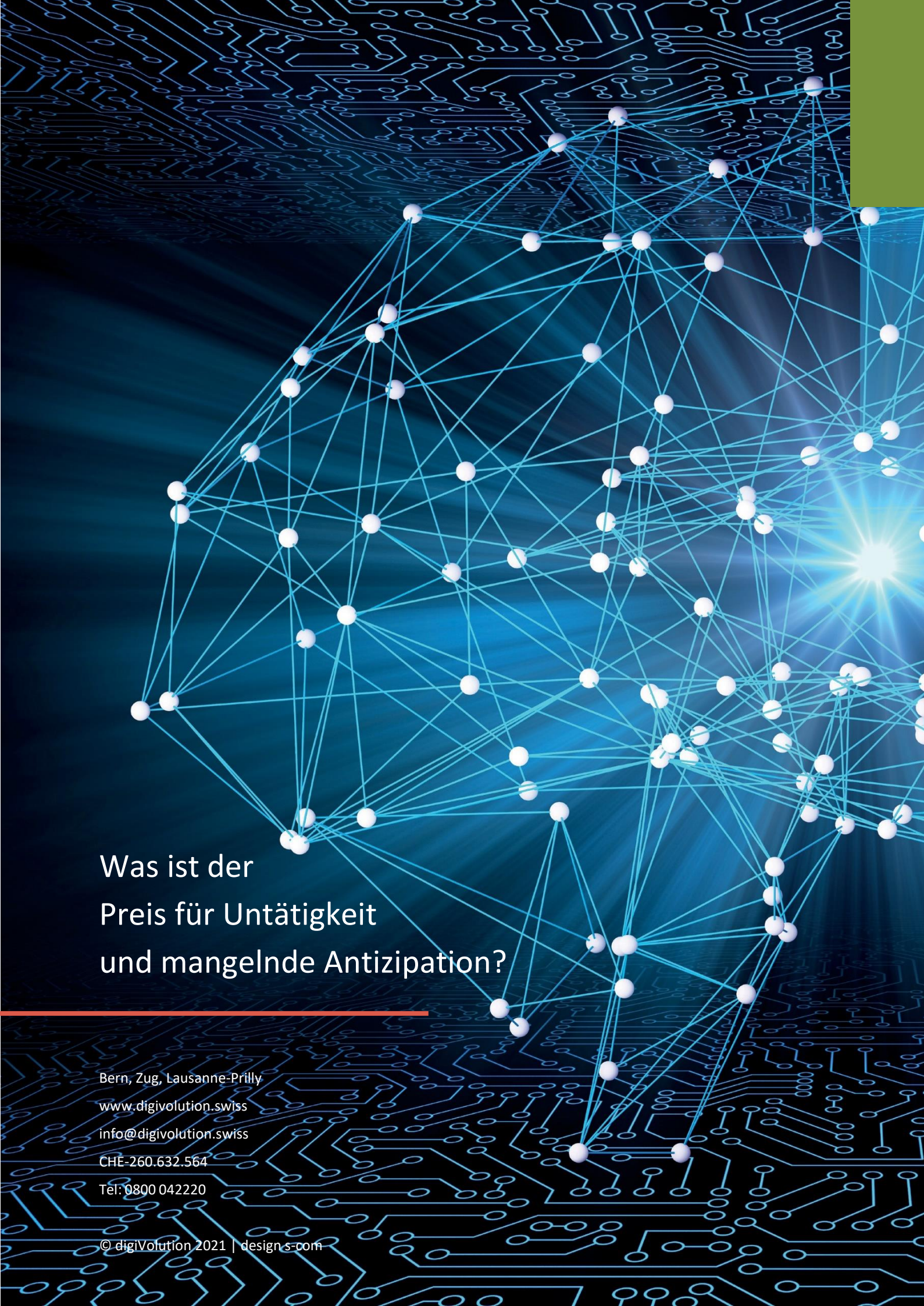
Porträt der Stiftung *digi*Volution

«Sinn und Sicherheit in einer cyber-bio-physikalischen Gesellschaft im Wandel»

*digi*Volution wurde 2020 gegründet und dient Entscheidungsträgern aus Politik, Wirtschaft und Wissenschaft als Beobachtungsstelle für das digitale Umfeld, vorsorgt sie mit Analysen, Beratung und Schulungen und trägt zum öffentlichen und politischen Dialog in der Schweiz über die Bedeutung und Sicherheit der digitalen Gesellschaft bei.

*digi*Volution will die Schweizer Gesellschaft dabei unterstützen, die vielfältigen und dynamischen Herausforderungen der Digitalisierung zu verstehen und zu meistern, damit sie rechtzeitig die richtigen Entscheidungen für ihre Sicherheit und ihren Wohlstand treffen kann.

*digi*Volution stützt sich auf unabhängige und neutrale Experten. Ihre Kritik ist konstruktiv. Ihre Methode ist ganzheitlich, systemisch und im Verbund. Sie sind überzeugt, dass Erfahrung und Antizipation Schlüsselelemente sind. Sie denken in einer strategischen und langfristigen Perspektive. Ihr Handeln basiert auf der Konvergenz von Unterschieden, Generationen sowie kybernetischen, biologischen und physikalischen Räumen.



Was ist der Preis für Untätigkeit und mangelnde Antizipation?

Bern, Zug, Lausanne-Prilly

www.digivolution.swiss

info@digivolution.swiss

CHE-260.632.564

Tel: 0800 042220