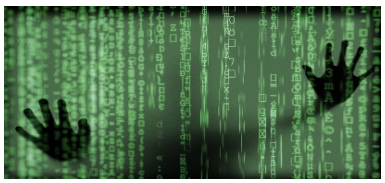
Corona-Pandemie, Ukraine-Überfall, Cyberkrieg – Gelingt der Schutz vor neuen Herausforderungen?

Vortragender: **Prof. Dr. Rainer B. Pelka**, Universität der Bundeswehr München, Neubiberg;
Leiter des Forschungsinstituts **IAS** (Institut für Angewandte Systemforschung, Unterföhring)[1]



Quelle: Pixabay (Aufruf: 23.11.2022)

***Corona* und *Ukraine* beherrschen seit 3 Jahren die Diskussion. Dies verdeckt die dritte große Gefahr, den *Cyberkrieg*. Alle drei Bedrohungen treffen uns unvorbereitet.**

Wir reagieren nur, und auch noch spät und einseitig. Öffentlich unterschätzt wird die *Cyber-Bedrohung*. Fast die Hälfte aller Firmen sehen ihr Unternehmen nach einem Cyberangriff existenzgefährdet.

1 Aktuelle Sicherheitsbedrohungen

Mit Trump (Überraschende Wahl 2016) und Putin (Krim-Annexion 2014 und versuchte Wahlmanipulation in den USA) geriet der [1]*Cyberkrieg* in den Blickwinkel nicht wirklich gelöster Probleme. Die [2]*Corona-Pandemie* (2020 bis heute) krempelte für über zwei Jahre unseren Alltag gründlich um. Und geradezu als Schock erlebten wir den [3]*Ukraine-Überfall* durch Putin am 24. Feb. 2022.

Was ist diesen drei Bedrohungen gemeinsam? Und lassen sie sich beherrschen? Unser Jahresthema „*Wie wollen wir leben*?“ unter dem heute diskutierten Aspekt „*Sicherheit*“ legt mindestens folgende drei Fragen nahe, die weitere Fragen zur Folge haben:

1)	Wie wollen wir leben?	Am liebsten wie bisher! Oder geht es noch besser?
2)	Wie können wir leben?	Ist unser Wollen noch relevant angesichts der sich abzeichnenden Bedrohungen?
3)	Was müssen wir ändern?	Müssen unsere Strategien dann nicht, um Ziel 1) unter der Bedingung 2) zu ermöglichen, unerwartete Ereignisse früher und schneller berücksichtigen?

Wenn ja, dann haben wir ein Problem. Denn dies ist uns bei allen drei o.g. Bedrohungen bisher nicht besonders gut gelungen, wie nachfolgend (s. Sc. 2) skizziert wird. (Re)Aktionen, auch einschneidende, gab es viele, vor allem bei Corona. Aber Aktionismus allein hilft nicht nachhaltig. Selbst seriöse Lösungsansätze bleiben riskant, wenn sie auf Konstanz oder zumindest weitgehender Stabilität der Randbedingungen basieren. Dies war lange Zeit, z.B. im Nachkriegsdeutschland mit einem über viele Jahre weitgehend stabilem Wohlstandszuwachs eine erfolgreiche Strategie.

Den o.g. Bedrohungen war gemeinsam, dass sie unerwartet auftraten. Reaktive Ansätze, d.h., „*wenn das Kind in den Brunnen gefallen ist*“, können den ersten Schaden nicht verhüten, und oft auch noch mehrere danach nicht. Das müssten sie aber, wenn wir verhindern wollen, dass wir eines Tages den Gesamtschaden nicht mehr bewältigen können. In welche Richtung ein wirklich präventiver Ansatz gehen muss, sei holzschnittartig anhand der o.g. Herausforderungen erläutert.

2 Schwachstellenanalyse der reaktiven Strategien

Auf alle genannten Bedrohungen reagierte die Gesellschaft, speziell die Politik, erst nach Überschreiten einer Schmerz-Schwelle und primär symptombezogen. Dadurch verschenkt man entscheidungsrelevante Informationen. Belegen lässt sich das an den Bedrohungen von Sc. 1.

Corona: *Events*: Wie reagierte die Politik? Lockdown1 (Schließung von Geschäften, Schulen, Events) im Mrz. 2020 anhand der *Inzidenz (= Überschreiten einer bestimmten Quote neu infizierter Personen)*. Lockdown 2 im Dez. 2020, ohne verbesserte Strategie. 2021/22: Durch „*Impfchancen*“ verbesserte Möglichkeiten, im Übrigen vermisste man veränderte oder gar verbesserte Strategien.

[1] Mail: pelka@ias-muenchen.de; Vortragsbearbeitung: Prof. Dr. Rainer Pelka (Unterstützung durch Frau Ass. jur. Eva Ditt).

Analyse: Der von den politisch ausgewählten Virologen in enger Abstimmung mit der Politik gewählte Ansatz zur Steuerung des Corona-Geschehens war engagiert, aber zu eingeschränkt und nur auf einen Lösungsansatz fixiert. Tatsächlich gab es alternative Strategien. *Schweden*, trotz internationaler und innergesellschaftlicher Kritik weniger restriktiv und stärker Risikogruppen-orientiert, war Nutznießer. Eine Beachtung solcher empirischen Befunde (v.a. im High-Risk-Bereich) und eine Min-Risk-Strategie unter Einbettung der falsch-positiven Risiken und ihrer Kosten hätte die finanzielle Belastung und die Nachteile für die Bevölkerung im Mittel deutlich verringern können (s. Pelka 2021).

Ukraine: *Events*: Zumindest in Deutschland hielten die meisten noch Mitte Februar 2022 einen russischen Einfall in die Ukraine für ausgeschlossen. Die Regierung verweigerte daher trotz dringender Bitten jegliche Waffenlieferungen in Nicht-NATO-Staaten, also auch in die Ukraine. Der Schock am 24. Feb.22, dem Tag des russischen Angriffs auf die Ukraine, war entsprechend tief.

Da wirkte das *100 Mrd.-Aufrüstungsversprechen* für die Bundeswehr durch den Kanzler kurz nach dem Überfall der Russen wie ein Befreiungsschlag. Doch die Umsetzung der Waffenlieferungsversprechen wie auch der BW-Aufrüstung in den Folgemonaten erfolgte unvollständig und schleppend, so dass inzwischen der praktische, erst recht der psychologische Effekt fast wieder verloren gingen.

Analyse: Der Überfall auf die Krim und deren Annexion 2014 hätte uns warnen können. Die nachfolgend andauernden Kämpfe in der Ostukraine hätten sogar warnen müssen. Spätestens die Einkreisung der Ukraine durch Truppenverlegungen an die Ost- (Donbass) und die Nord-(Weißrussland) Grenze hätte einen Abbau bestehender Abhängigkeiten erfordert. Stattdessen wurde nach *Nord stream 1* mit *Nord stream 2* zu Beginn 2022 die geplante Abhängigkeit von russischer Energie sogar noch erhöht.

Auch der Aufrüstungseffekt hielt sich in Grenzen. Tatsächlich wurden den Ukrainern zunächst weder die versprochenen Verteidigungswaffen geliefert noch die Schlagkraft der Bundeswehr nennenswert verbessert. Bis heute überzeugt Deutschland mit der Umsetzung der Scholz-Ankündigung nicht, die Ukraine nicht, die Bundeswehr nicht und auch nicht die Weltöffentlichkeit. Die Ukraine hatte sich mehr zeitnahe Hilfe erhofft. „*Die Politik schmückt sich gerne mit Worten, aber für die Geschichte zählen nur die Taten*“.

Cybersicherheit: *Events*: Politik und IT-Sicherheitsunternehmen sind immer wieder aufs Neue irritiert von Whistleblowing[2] oder erfolgreichen Cyberangriffen. Zwar reagiert man bei Bekanntwerden bestehender Schwachstellen schnell und meist auch wirksam, aber das Risiko unerwarteter Crashs bleibt bestehen. Die Schadenssummen steigen von Jahr zu Jahr und kommen längst in einen kritischen Bereich. Dies belegen folgende Aufwands- und Schadensbeispiele:

Weltweite Schadensentwicklung 2007 bis 2022: Zwar sind die genauen Schadensentwicklungen nicht bekannt, weil Unternehmen und auch staatliche Organisationen solche Zahlen nicht gerne veröffentlichen, dies oft auch gar nicht genau können. Umfragen und einige spektakuläre Fälle geben jedoch einen Anhaltspunkt zur zeitlichen Entwicklung der Schadenshöhe:

1) Der Hackerangriff auf das HEARTLAND Payment System 2008 verursachte einen Schaden von ca. ..... 0,1 Mrd. $
2) Die Kosten des Whistleblowings von Snowden 2012 verursachte – kaum schätzbar – einen Schaden von ca. ... 1 Mrd. $
3) Beim Hacken von eBay 2014 geht man (154 Mio. Kd.-Daten a 700$ pro Fall) von einem Schaden aus von ca. ..... 10 Mrd. $
4) Der Schaden durch Cambridge Analytics, der 2016 evtl. Trump zur Präsidentschaft verhalf, könnte sein. .... 100 Mrd. $

Analyse: *Aufwandsentwicklung für IT-Sicherheit (in D):* Lagen die Kosten für IT- Sicherheitsaufwendungen 2007 noch im Mio. Bereich, so wuchs dieser, nicht zuletzt aufgrund spektakulärer Schadensfälle in 2012 auf ca. 1,5 Mrd. €. Im Jahr 2017 hatte sich auch dieser Wert mit 3,7 Mrd. € ehr als verdoppelt, 2022 erneut verdoppelt auf 7,8 Mrd. €. Bis 2025 wird ein weiterer Anstieg auf 10,3 Mrd. € geschätzt (Quelle Statista; Okt.22[3]).

---

[2] Ein wichtiges Beispiel ist die Einflussnahme auf die Wahlen in GB und in den USA 2016 durch Cambridge Analytica, die für die Öffentlichkeit unerwartet Donald Trump an die Macht brachte (s. Abschlussbericht der Datenschutzbehörde: „*Nein, der Analytica-Skandal fällt nicht in sich zusammen*“ (netzpolitik.org, 23.10.2020).

[3] Nach einer Umfrage der FH Bielefeld hatten bereits 2019 60% der Unternehmen in D ein spezielles IT-Sicherheitsbudget, welches zwischen 2% und 6% des IT-Budgets ausmacht. Von Experten als sinnvoll erachtet werden ca. 14% des IT-Budgets (Stand: 2022).

Schadensschätzung 2022 für Deutschland: Dass diese Aufwendungen bei weitem nicht ausreichen, zeigt sich an den tatsächlichen Schadensfällen. So berichtet Statista von einem berichteten Gesamtschaden durch IT-Angriffe in D in Höhe von 203 Mrd. €[4], also das 25-fache der Aufwendungen. Um diese Schadenshöhe zu verdeutlichen, sei in Erinnerung gerufen, dass der gesamte Bundeshaushalt 2022 nur knapp 460 Mrd. €, also nur wenig mehr als das Doppelte davon betrug.

Politik und Öffentlichkeit, auch IT-Fachleute glauben, keine andere Möglichkeit zu haben, als „*kritische Ereignisse*" abzuwarten und dann möglichst schnell erkannte Schwachstellen zu beseitigen. Vor dem Hintergrund solch dramatischer Entwicklungen sind wir aber aufgefordert, nach alternativen Sicherheitsmöglichkeiten zu suchen!

3 Evidentes Präventionspotential bei sensiblem Risikobewusstsein

Suchen wir nach besseren Lösungen, sollten wir den Blickwinkel verändern, um das evidente Präventionspotential zu aktivieren. Der unbestreitbare Satz „*Zukunft lässt sich nicht zuverlässig extrapolieren, mithin können singuläre Ereignisse nie ausgeschlossen werden!*" verführt dazu, uns auf unser reaktives Handlungspotential zu konzentrieren. Tatsächlich gibt es zwischen den Extremen „*Alles Mögliche tun*" und „*Nichts tun*" sinnvolle Zwischenstufen, die für die hier genannten „*unerfreulichen Ereignisse*" beispielhaft skizziert werden. Dass Versicherungen selbst bei weniger beeinflussbaren Events wie Naturkatastrophen dies können und trotzdem überleben, sollte uns veranlassen, den Sachstand im Hinblick auf alternative Steuerungsmöglichkeiten genauer zu analysieren.

Corona

Evaluation: Ein Lockdown ist – ebenso wie der totale Einsatz der zum Glück schnell entwickelter Impfstoffe (Impfpflicht) – eine Maximalstrategie, um das Risiko einer Covid-Erkrankung, ja allein schon einer Corona-Ansteckung, möglichst zu 100% zu verhindern. Diese lässt außer Acht, dass eine solche Maßnahmen nicht nur hohe direkte Kosten, sondern durch das Ignorieren möglicher Alternativen sogar noch viel höhere Kosten verursachen kann, wenn die Nebenwirkungskosten („*Kollateralschäden*") wie z.B. „*Zahl der nicht Getesteten/Nicht Geimpften/Nicht im Lock-down Befindlichen zu minimieren*" höher werden als der Zusatznutzen. Dies hat auch im Falle Corona vermeidbare, erhebliche Mehrkosten verursacht, vor allem bei Kindern und Jugendlichen.

Tatsächlich wäre es nicht zu schwer, – die wissenschaftliche Statistik[5] bietet hier ein leistungsfähiges Instrumentarium an – den erwarteten (Mehr)Nutzen bzw. Mehrschaden zusammen mit den Eintrittswahrscheinlichkeiten ausreichend gut zu schätzen, um eine – wenn nicht optimale, so doch im Ergebnis viel vernünftigere – Entscheidung zu ermöglichen (s. Pelka 2021).

Es gab ergänzende Alternativen zu den Labor- und Labor-Schnelltests. Zum Beispiel hätte es der von Pelka (2020) entwickelte klinische Schnelltest ***CorK*** erlaubt, über das Internet fast kostenlos und mit beliebiger Wiederholungsmöglichkeit den Test valide einzusetzen. Jeder Interessierte hätte rechtzeitig Risiken besser einschätzen und ggfls., z.B. ggü. Verwandten und Freunden, verringern können.

Perspektive: ***CorK*** könnte auch in Zukunft – mit leicht und preiswert adaptierbaren Modifikationen – dazu beitragen, Varianten des Corona-Virus oder selbst anderer Viren mit krankheitsauslösendem Potential zu identifizieren und lokal gezielt angemessene Maßnahmen zu ergreifen, wenn dies geboten erscheint. Generell würde dies erfordern, neben Diagnose und Therapie den Risikobegriff stärker in gesundheitsbezogenen Steuerungskonzepte einzubeziehen.

---

[4] Umfrage von 10.Jan. -13.Mrz.2022 bei knapp 1.000 Firmen in D mit mindestens 10 Mitarbeitern: Um einen Hinweis auf die Aufteilung dieser Schäden zu bekommen, sei (bezogen auf die Befragung Jan-März 22) eine prozentuale Aufteilung gegeben: [1]Diebsstahl/Schädigung 21%, [2]Umsatzeinbußen 20%, [3]Plagiate/Patentverletzung 19%, [4]Imageschaden 12%, [5]Zusatzmaßnahmen 9%, [6]Rechtsstreit 8%, [7]Sonstiges 11%; (Summe 100%).

[5] *Wissenschaftliche Statistik* meint nicht nur das Ermitteln und Präsentieren von geeignet aufbereiteten Daten, sondern auf der Basis von Theorien oder empirisch gestützten Modellen durch Einsatz methodisch leistungsfähiger Verfahren (incl. IT) die Erhebung, Dokumentation, Kontrolle und Hypothesengeleitete Analyse von Daten zum Zwecke der wissenschaftlichen Erkenntnis zu leiten, ggfls. auch des praktischen Nutzens, wenn diese Hypothesen praxisrelevant sind.

Ukraine

Evaluation: Warum hätten wir uns auf das Problem Ukraine anders vorbreiten sollen? Schließlich war zumindest Deutschland der Ukraine als ehemaligem Teilstaat der Sowjetunion nicht verpflichtet. Und bei dem ambitionierten Vorhaben, die weitere Klimaänderung zu bremsen, ohne den eigenen wirtschaftlichen Erfolg zu gefährden, schien eine Energiequelle, die auf längere Zeit fast unerschöpfliche Reserven zu haben schien, als Übergangslösung attraktiv.

Natürlich ist eine politische Entscheidung zu einer Entwicklung verringerter Abhängigkeit von einem Staat mit Mehrkosten verbunden. Und solange das Risiko eines Lieferstopps vernachlässigbar erschien, war eine vermeintliche Risikoverteilung mit deutlich höheren Kosten den Wählern nicht leicht vermittelbar. Umso wichtiger ist eine rechtzeitige und angemessene Evaluation von Risiken. Und diese Risiken waren spätestens seit 2014 nach der Krimannexion durch Russland nicht mehr vernachlässigbar.

Perspektive: Trotz aller inzwischen erkennbaren Zielsetzung von Russland und auch von der VR China mit seinen Drohungen einer notfalls auch gewaltsamen Übernahme von Taiwan („*Heim ins Reich*“) ist bisher (*Stand: 13. Juni 2022*) seitens Deutschlands die Abhängigkeit von China betreffend noch keine Strategieänderung erkennbar.

Ob die inzwischen geplanten und umgesetzten Maßnahmen zur Verringerung der Russlandbezogenen Gas-/Energieabhängigkeit ausreichend sind, wird sich noch zeigen müssen. Experten melden schon jetzt begründete Zweifel an, vor allem für den Winter 23/24, wo es dann in D nach ggw. Planung keine AKWs mehr gibt, was im ggw. politischen Aktivismus noch keine Rolle zu spielen scheint.

Cybersicherheit

Evaluation: Cyberrisiken wurden lange massiv und selbst heute noch essentiell unterschätzt. Dafür gibt es viele Gründe. Es trifft oft andere („*Heiliger St. Florian, verschon‘ mein Haus, zünd andere an!*“), viele Schäden werden geheim gehalten, weil ihre Kenntnis Vertrauen in das Unternehmen bzw. die betreffende Institution verringern könnte. Und sie sind nicht ganz leicht zu quantifizieren, weil die wahren Kosten nicht sofort entstehen oder lange unsichtbar bleiben.

Perspektive: Wie die Umfrage von *bitcom* zeigt, erwarten die Firmen in Zukunft aber verstärkte Cyberangriffe, und zwar vor allem auf ihre kritische Infrastruktur. Und nicht nur das, 45% der Unternehmen fürchten inzwischen aufgrund dieser vermehrten Angriffe um ihre Existenz (Quelle *bitcom*, 31.08.2022). Leider wird auch das Eintrittsrisiko nicht geringer. Müssen wir nicht doch unsere, bisher nur reaktive Strategie ändern? Und können wir das überhaupt?

Im Folgenden beschränke ich mich auf das Thema Cybersicherheit. Hier lässt sich leichter aufzeigen, welche Veränderungen im Einzelnen notwendig und zugleich möglich sind, um unerwarteten Bedrohungen früher und wirksamer, zugleich nachhaltiger und doch sparsamer zu begegnen. Grundsätzlich könnten aber die formulierten Überlegungen und die vorgestellten Konzepte auch auf andere Bedrohungsszenarien angewandt werden, wie zum Beispiel die anfangs mitdiskutierten Ereignisse „*Corona*“ und „*Ukraine-Überfall*“.

4 Siegeszug der IT-Revolution und deren Kollateralschäden

Der Siegeszug der Computer Technologie begann im 2. Weltkrieg, war aber wegen seiner räumlich und finanziell kostspieligen Technologie (Röhren-, später Transistoren-Technik) auf wenige Nutzer beschränkt. Erster Schritt auf dem Weg zu einem Gebrauchsgegenstand war die Entwicklung der *Halbleitertechnik* und der sog. *Personal Computer* (PCs) in den 70ern. Doch Informationsübertragung war schwierig, weil jeder Hersteller eigene Verschlüsselungen der zu transportierenden Information hatte. Der Nutzen einer Vereinheitlichung wurde schon in den 70ern erkannt, aber erst in den 90ern umgesetzt. Jetzt war die Grundlage des *Internets* und der *IT-Technologie* geschaffen.

Zwar konnte man schon in den 80ern nach dem Siegeszug des „*PCs für Jedermann*“ und noch stärker in den 90ern beim Mobiltelefon, dem „*Handy für Jedermann*“ ahnen, dass sich die Welt durch die neuen Techniken verändern würde, aber weder war die Geschwindigkeit der Entwicklung noch die Macht ihrer kommerziellen Entwickler vorauszusehen. Freaks und ihre Anhänger sprachen von einem neuen „*goldenen Zeitalter*“.

Doch bald zeigten sich auch die Schattenseiten dieser Entwicklung. Das am schnellsten sichtbare Problem war die Sorge vor dem „*gläsernen Menschen*“. Zwar wurde von der Mehrheit der Nutzer die Gefährlichkeit des Problems lange unterschätzt (der Abruf der Internetleistungen kostete ja nichts), aber zunächst die Wissenschaft warnte frühzeitig vor den Risiken. Spektakuläre Enthüllungen und zahllose Beschwerden bis hin zu aufwendigen Gerichtsverfahren veranlassten schließlich auch die Politik, nach Lösungen für einen größeren Schutz des Einzelnen zu suchen.

Sie mündeten in mehrere Gesetze und Verordnungen, von denen die europäische Datenschutz-Grundverordnung (=DSGVO) bei uns am bekanntesten wurde. Doch zeigt sich auch hier, dass eine Problemlösung nicht einfach ist. Viele beschweren sich, dass das Gesetz von den Großunternehmen, insbesondere den außereuropäischen, unterlaufen wird, andererseits kleine Unternehmen und der Privatmann sowie insbesondere die Forschung erheblich eingeschränkt werden und zugleich viel mehr Aufwand haben. Kritischer noch ist die Tatsache, dass ein perfekter Datenschutz gar nicht möglich erscheint, weil die heutige Technik und die sie nutzende Gesellschaft nicht mehr in der Lage sein dürfte, ausreichend Sicherheitsvorkehrungen zu treffen (s. Sc. 1).

Inzwischen ruht die Hoffnung auf der *Künstlichen Intelligenz (**KI**),* die – zunächst kaum bemerkt – inzwischen in vielen Unternehmen und auch staatlichen Organisationen Einzug gefunden hat. Doch auch hier gibt es Probleme. Denn wir hoffen, dass die KI das tut, was wir wollen. Und tatsächlich müssen wir uns wieder – wie bei der Industrialisierung im 19. Jh. – dem Takt der KI unterwerfen. Es wächst die Sorge, dass die KI uns irgendwann beherrscht und überflüssig macht.

Selbst im Bereich ***Sicherheit*** bietet **KI** nicht nur Chancen, sondern auch zusätzliche Risiken: Zum einen kann man nie ganz sicher sein, dass durch **KI** in falschen Händen nicht gerade das verschärft wird, was verhindert werden soll, nämlich unberechtigtes Ausspionieren oder Zerstören, zum andern kann selbst der bisherige **KI-Einsatz** nicht verhindern, dass es immer wieder zu erfolgreichen Hacker-Angriffen o.ä. kommt.

Daher bedürfen dringender Antworten Fragen wie diese:

- Lässt sich der Antagonismus von Schutz und Freiheit vertretbar lösen?
- Lässt sich **KI** so einsetzen, dass sie wirklich den Menschen darin unterstützt, geschützter und zugleich human zu leben?

Victor: In den folgenden vier Sektionen (Sc. 5-8) werden *notwendige oder zweckmäßige Anforderungen an ein künftiges Security-System* formuliert, deren Umsetzung die drohende Entwicklung im Cyberkrieg verhindern kann. In ähnlicher Weise sollte eine Lösung mit entsprechender Adaption auch bei den Bedrohungen „*Corona*“ bzw. „*Ukraine*“ nützlich sein können.

Ich behaupte, dass es attraktive, funktionierende Lösungen für die bisher diskutierten offenen Probleme gibt. Die Lösung der o.g. Fragen bezeichne ich kurz als **VICTOR©**, ein Akronym für

- „*Value based, Interactive, Cognitive by Teaching, Open Response System*“ (Wertebasierter, interaktiver Lernautomat mit selbstevaluierender Künstlicher Intelligenz).

VICTOR© scheint zunächst nur eine vage Idee zu sein. Diese wird aber in den folgenden Sektionen Sc.5 bis 8 mit mächtigen Konzepten gefüllt. Seine hier dargestellte Hauptzielsetzung ist die ***Verbesserung der Security*** durch schnellere Anpassung an neue Risiko- Situationen oder – Entwicklungen.

5 Unabhängigkeit von externer Evaluation durch drei Qualitäten (Q1-Q3)

Was ist denn VICTOR[6]? Es genügt, wenn ich VICTOR als **komplexen Algorithmus** beschreibe, der aufgrund des aktuell bestehenden Zustands **Z** zu jedem Input **X** einen bestimmten Output **Y** erzeugt.

In Abhängigkeit von den tatsächlichen Umweltkonsequenzen (also dem nachfolgenden Input) verändert sich nicht nur die Funktion **g**, sondern auch **f** und – algorithmisch bestimmt – unter bestimmten Bedingungen auch die Struktur von Z (die Evaluationsgrundlage), X (die Abbildung des Inputs X' in VICTOR) und Y (die Reaktionsklassifizierung von VICTOR) (**s. Abb. 1**).

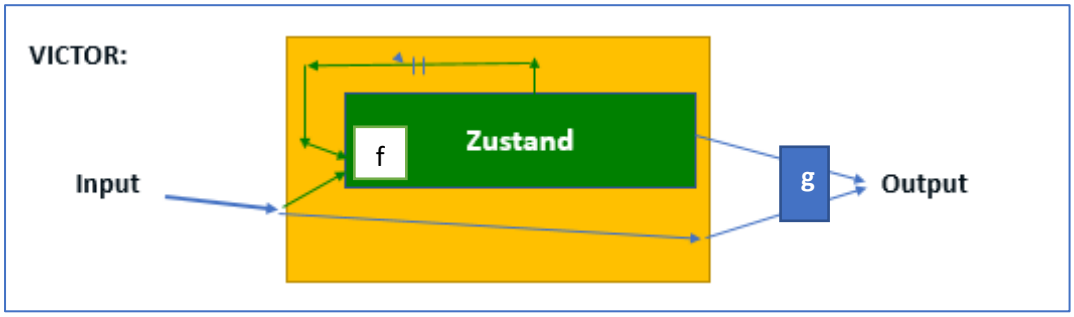


Abb.1: VICTOR, definiert durch Zustand **Z**, Input **X** und Output **Y** zu jedem Zeittakt t (t = 1,2, ...) wird beschrieben durch die **Ergebnisfunktion** $g = g_t$ mit $Y_t = g_t (X_t, Z_t)$ und die **Überführungsfunktion** $f = f_t$ mit $Z_t = f_t (X_t, Z_{t-1})$. Die Event-Folge $E_t=(X,Y,Z)_t$ beschreibt die Entwicklung und Umwelt-Interaktion von VICTOR.

Als Algorithmus ist VICTOR natürlich programmierfähig und in seinen zentralen Aspekten auch bereits erfolgreich programmiert. Zentral sind bei VICTOR folgende drei Qualitäten:

- **Q1)** **Stochastische Beziehungen**: Die Beziehung g „*Ergebnisfunktion*" zwischen Input (Stimulus) X und Output (Reaktion) Y bei bestehendem Zustand Z ist stochastisch, d.h. die Zuordnung erfolgt nach Wahrscheinlichkeit. Gleiches gilt für die Beziehung f „*Überführungsfunktion*" zwischen Input (Stimulus) X_{t-1} und vorausgehendem Zustand Z_{t-1}.
- **Q2)** **Selbstevaluation**: VICTOR evaluiert den „*Erfolg*" der von ihm gewählten Zuordnung zwischen Input X und Output Y unter spezieller Zustandsbedingung Z selbständig ohne externe Instanz.
- **Q3)** **Erfahrungsbasierte Änderung der Struktur von Z**: Änderungen von Z, X und Y erfolgen aufgrund einer internen Bewertung des *tatsächlichen*, nicht des *erwarteten Erfolgs* der gewählten Reaktion Y von VICTOR auf seine Wahrnehmung X des Umwelt-Stimulus X'.

Was bedeuten diese drei Kernqualitäten **Q1** bis **Q3** in der Praxis?

Q1 bedeutet, dass der (elementare) Lernprozess durch *Ändern der Reaktionswahrscheinlichkeiten* erfolgt, *Erhöhung* nach „Belohnung/Erfolg" und *Verringerung* nach „Bestrafung/Misserfolg".

Q2 bedeutet *die interne Evaluation*, d.h., dass die Grundlage dieses Lernprozesses nicht von einer externen Instanz, sondern allein von VICTOR selbst abhängig ist. Das heißt nicht, dass der Lernprozess von der Außenwelt völlig unabhängig wäre. Denn wenn deren Reaktion von VICTOR als nachteilig/schmerzhaft (~Zustandsverschlechterung) erlebt wird, hat dies auch Einfluss auf den Lernprozess, aber eben nicht unmittelbar, sondern erst über die Selbstevaluation des Systems.

Q3 präzisiert diesen Lernprozess der „*Erfahrungsbasierte Entwicklung der inneren Struktur* von Z, X und Y" d.h. die Struktur von Z nimmt mit der Zeit die Komplexität an, die erforderlich ist, um den Umweltbedingten Anforderungen möglichst ausreichend zu entsprechen (s. Pelka 2022,2017,1979,1975).

---

[6] Leider ist eine genauere Beschreibung notwendigerweise mathematisch, aber das Verständnis der wesentlichen Aspekte setzt nicht das Verstehen aller mathematischen Details voraus. Formal gesehen ist VICTOR ein sog. MOORE-Automat, der für jeden Zeittakt t (t = 0,1, 2, ...). beschrieben wird durch ein Ereignis $E_t = (Z_t, X_t, Y_t)$. Die Folge E_t (t= 1, 2, ...) beschreibt sowohl seine Struktur als auch seine Interaktion mit der Umwelt (Pelka (1975)..

Dabei wird dessen Output (=Reaktion) Y_t zum Zeitpunkt t vom eingehenden Input (= wahrgenommener Stimulus) X_t und seinem aktuellen (inneren) Zustand Z_t stochastisch bestimmt. Sein Zustand Z_t zum Zeitpunkt t wird wiederum vom vorausgehenden Zustand Z_{t-1} und dem aktuellen Input X_t auch stochastisch bestimmt (Pelka 2017,1975).

6 Anpassung bei geänderten Bedingungen durch Differenzierung (Q4)

Ein typischer elementarer Lernprozess, auf dem auch viele **KI**-Modelle beruhen, ist programmiert als „*Erhöhung der Eintrittswahrscheinlichkeit*“ der extern akzeptierten Outputs (Reaktion) auf bestimmten Input (Stimulus) im nachfolgenden Takt.

- *Erste Schwachstelle* dieses Ansatzes, zum Beispiel gegenüber natürlichen menschlichen Lernprozessen ist, dass sich Bewertungssysteme und folglich die sich daran orientierenden, konkreten Bewertungen ändern können, z.B. wenn die **externe Instanz** sich ändert (*anderer Lehrer*) oder selbst neuen Bedingungen (*veränderte Anforderungen*) unterliegt. Darauf können die ggw. programmierten KI-Systeme nicht eigenständig effizient reagieren.
- *Zweite Schwachstelle* ist das *Fehlen einer sinnvollen Generalisierung*. Eine Stimulus-Situation ist nie mit einer anderen identisch. Während menschliche Lerner anfangs nur grobe Klassen unterscheiden, lernen sie mit der Zeit, anforderungsbezogen differenzierter zu reagieren. Das aber lässt sich allein mit dem Stimulus-Response-Schema, wie dies z.B. die Psychologen Pawlow oder Skinner und deren „Schulen“ versuchten, nicht mehr abbilden.

Auch hier besitzt VICTOR einen Algorithmus der zielbezogenen *Differenzierungsfähigkeit (**Q4**)*. Dieser wird wirksam, wenn sich (anhand formaler Kriterien) zeigt, dass eine bestimmte Reaktion (Output) nicht für alle Elemente einer bestimmten Stimulus-Klasse gleich gut geeignet ist. Dadurch gelingt VICTOR eine Differenzierung dort, wo sich dies als sinnvoll erweist.

Ein attraktives Anwendungsbeispiel für den Nutzen dieses Differenzierungsalgorithmus ist die sog. *Verhaltensformung*, die zum Beispiel von Dompteuren (bei der *Tierdressur*) und bei Psychologen (z.B. in der *Verhaltenstherapie*) bei anfänglichem Fehlen geeigneter Reaktionsmuster sehr erfolgreich eingesetzt wird.

7 So komplex wie nötig, so einfach wie möglich durch Verschmelzung (Q5)

Der Anpassungserfolg von VICTOR, der in Sc. 6 skizziert wurde, erzeugt automatisch ein anderes Problem, mit dem heute sämtliche hoch zivilisierten Gesellschaften zu kämpfen haben, nämlich dem Problem der *Überkomplexität*.

Dem begegnet VICTOR mittels eines weiteren Algorithmus durch eine *automatische Strukturvergröberung (**Q5**)*, wenn dies geboten ist. Dieser *Verschmelzungs-/Vereinfachungs-Algorithmus* ist reversibel, z. Bsp., wenn sich ändernde Bedingungen eine erneute Differenzierung sinnvoll erscheinen lassen. VICTOR vermeidet dadurch, unnötige Strukturen beizubehalten. Seine Lösungswege bleiben dadurch problembezogen sparsam.

„*So einfach wie möglich, so komplex wie nötig*“: Jeder geplanten Differenzierung (Q4, s. Sc. 6) geht eine Prüfung möglicher *Komplexitätsreduktion* (Q5) voraus. Durch dieses Zusammenspiel von Differenzierung und Verschmelzung strebt Victor eine problemangemessene Komplexität an und erreicht sie in grundsätzlich möglichen Fällen auch.

Beispiele für eine sinnvolle Anwendung dieses Algorithmus ist auch wieder die Verhaltensformung. Interessant wären die mit der Zeit immer weiter wachsenden *Gesetzes-, Verordnungs- und sonstiges Regelungspakete,* die für deren Anwender Entscheidungen wegen des fortgesetzt ansteigenden Prüfungsbedarfs immer unhandlicher, zeitaufwendiger und unzuverlässiger machen.

Denn einmal aufgenommene Regelungen werden nicht, an der falschen Stelle oder viel zu spät aufgegeben. „*Zu spät*“ meint, dass sie eigentlich zur Lösung der anstehenden Entscheidungen nicht mehr erforderlich oder sogar unangemessen sind, aber aus formalen Gründen (weil sie noch rechtsgültig sind) berücksichtigt, zumindest geprüft werden müssen.

8 Risiko-Verringerung durch Mehrstufigkeit (Q6, Q7)

Zwar weist VICTOR schon mit den in Sc.5 bis 7 skizzierten Eigenschaften gegenüber üblichen IT-Schutzsystemen, auch den KI-gestützten, prinzipielle Vorteile auf, doch Sicherheits-entscheidend ist eine weitere Eigenschaft, die gerade bei neuen, bisher unbekannten Störeingriffen von großer Bedeutung ist. VICTOR besitzt eine *lernende Risiko-Evaluation* (Q6) und zusätzlich ein *mehrstufiges Sicherheitssystem* (Q7).

Lernende Risikoevaluation (Q6): VICTOR kann, wenn eine entwickelte Lernstruktur vorliegt, sowohl den *Zugang* (grundsätzliche Erlaubnis) als auch den *Verlaufs-Input* (Sicherstellen nur erlaubter Nutzerverhalten) an allen kritischen Stellen bezüglich sich abzeichnender Risiken evaluieren und in Abhängigkeit von dem Evaluationsergebnis handeln/reagieren. Dadurch kann Victor – aus der Erfahrung lernend – sich ständig verbessern.

Mehrstufigkeit (Q7): Ein mehrstufiges Verfahren stellt sicher, dass alle Inputs (Zugang oder bisherige Verlaufspfad) einer der drei Klassen zugeordnet werden:

- [1]*zulässig*, [2]*unzulässig* bzw. [3]*unklar*.

Gruppe 3 („*Unklar*“) wird (so lange) einem mehrstufigen Testen unterworfen, bis die Kontrolle mit ausreichender Sicherheit gegeben ist, dass es sich [nicht] um einen unerlaubten Zugang/ Pfad handelt. Unsichere Inputs oder Verläufe werden einer stärkeren Kontrolle unterzogen.

Effizienz: Obwohl bei VICTOR Zugriffe generell mehrstufig behandelt werden, ist das Vorgehen ökonomisch, weil nur die Events der mit jeder Stufe kleiner werdenden Gruppe 3 mehrfach geprüft werden. Dadurch wird es auch möglich, die jeweiligen Sicherheitsanforderungen an ein im Voraus bestimmbares Niveau anzupassen. Das Sicherheitsszenario ist insgesamt so aufgebaut, dass die Ökonomie der Abläufe und die Sicherheitsanforderungen in einem dynamischen Gleichgewicht verbleiben.

9 VICTOR, ein Quantensprung für den Security Bereich

VICTOR© (= **V**alue based, **I**nteractive, **C**ognitive by **T**eaching, **O**pen **R**esource System) ist ein programmierter Lernautomat mit selbst-evaluierender Künstlicher Intelligenz (**KI**). Mit geeigneter Anpassungsprogrammierung kann er als IT-Sicherheitssystem eingesetzt werden, das die in Sc. 5-8 beschriebenen Potentiale **Q1 bis Q7** besitzt und dadurch wesentliche Vorteile gegenüber den aktuell eingesetzten Schutz-Systemen aufweist.

Insbesondere kann VICTOR präventiv wirksam sein, weil er nicht erst nach einem Schadensfall an die neue Herausforderung angepasst werden muss, sondern aufgrund seines Lernalgorithmus schon bereits *Risiko-Ereignisse* ab ihrem ersten Auftreten berücksichtigt.

10 Quellenauszug:

Pelka RB (2022): VICTOR (Value based, interactive, Cognitive by Teaching, Open Response System). Problemlösungs-Algorithmus mit Anwendung als Sicherheitssystem. **IAS** -Unterföhring/München (unveröffentlicht).

Pelka RB (2021): Strategiesuche. Müssen wir – Corona geplagt – öfter bipolar denken? In: Forschung & Lehre, Bonn 5/21: 378-79.

Pelka RB (2020): CorK – Corona Klinischer Schnelltest; Differential-Diagnose, Risiko-Score und Empfehlungen. Kurz-Information zu Entwicklung, Anwendung und Gültigkeit (Version 3.0 vom 08.05.20). IAS-Unterföhring/München (unveröffentlicht).

Pelka RB (2017): MUPLA-Algorithmus: Programmierter Lernautomat zu Mustererkennung am Beispiel von Ziffern. IAS München (unveröffentlicht).

Pelka RB (1979): Experimentelle Lernspiele und ihre Simulation. *Carré, ein* Vergleich von Automaten- und menschlichem Verhalten. In Hrsg. H. UECKERT / D. RHENIUS: Komplexe menschliche Informationsverarbeitung. Beiträge zur Tagung ‚Kognitive Psychologie in Hamburg 1978. Huber Bern: 270-84.

Pelka RB (1975): Lernprozesse in Nicht-Markov'schen stochastischen Automaten (Inauguraldissertation), LMU Universität München.

❑