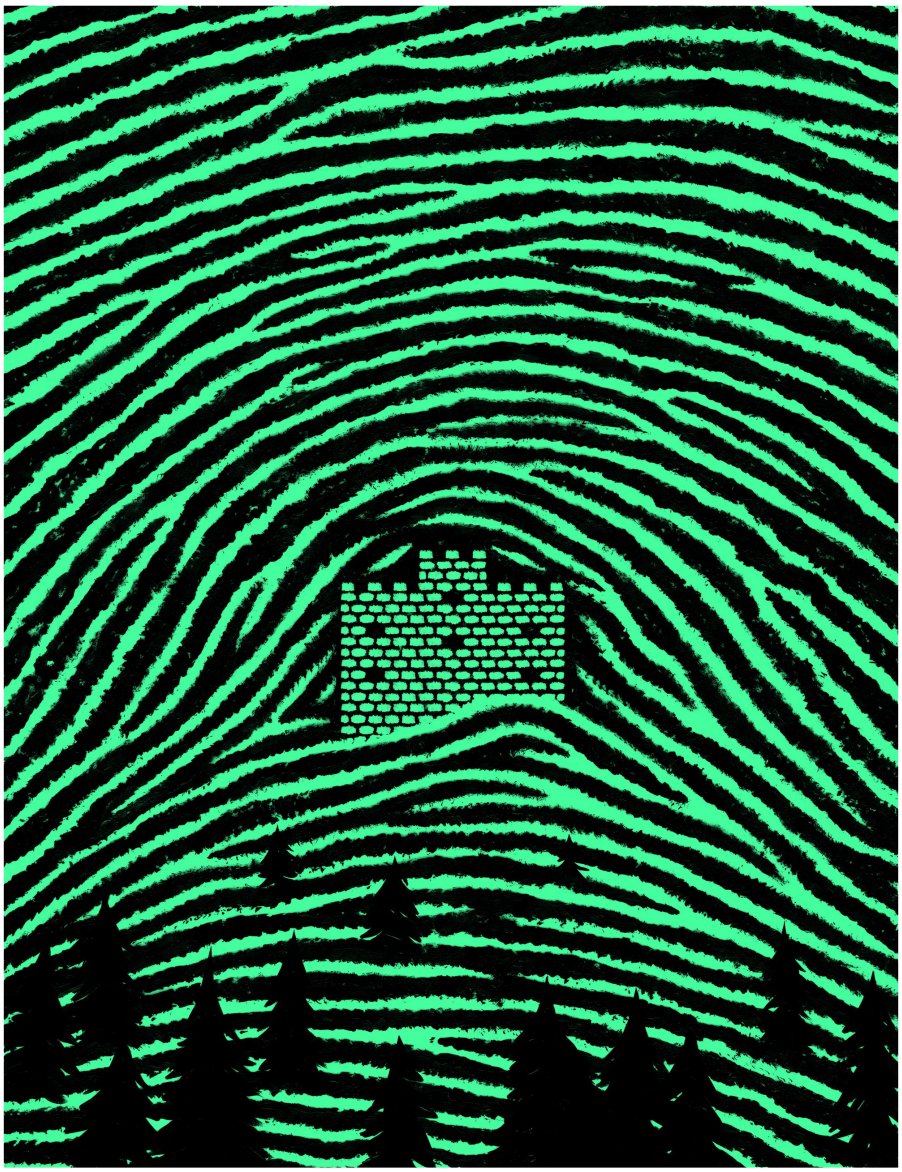
Wie sich das Internationale Rote Kreuz neu erfindet – und wie die Schweiz dabei verliert

Das IKRK etabliert sich als globales Labor für technische Innovationen. Das geschieht allerdings nicht in Genf, sondern in Luxemburg. Die Geschichte einer verpassten Chance.

Von Adrienne Fichter (Text) und Lina Müller (Illustration), 31.07.2023



Das Internationale Komitee vom Roten Kreuz sei zu bürokratisch, aufgebläht und habe zu viel Personal: Seit Monaten steht das IKRK in Genf in der Kritik. Weil die Hilfsorganisation ihr Jahresbudget von 2,8 Milliarden Franken nicht mehr stemmen konnte, kam es diesen Frühling zu einer Massenentlassung. In einem offenen Brief forderten Mitarbeiterinnen darauf eine Aufarbeitung der «Budgetverwendung». Und internationale Experten wie David Forsythe kritisieren die Orientierungslosigkeit der Führungsriege. Inzwischen bettelt die stolze Organisation beim Bundesrat um zusätzliche finanzielle Mittel.

Das IKRK – die wichtigste und renommierteste humanitäre Institution der Schweiz – durchlebt gerade eine schwere Krise. Was im medialen Lärm um die finanzielle Schieflage allerdings kaum Beachtung findet, ist die bemerkenswerte digitale Pionierarbeit, die das IKRK leistet. So soll das humanitäre Völkerrecht in die Zukunft gerettet werden. Oder genauer: in den Cyberspace.

Dabei geht es um Fragen von grosser Tragweite: Wo verläuft in einem Cyberkrieg die Grenze zwischen Zivilisten und staatlichen Akteurinnen? Was bedeutet der Claim aus dem IKRK-Leitbild «Leben und Würde schützen», wenn Menschen Opfer eines Krieges im Cyberspace werden? Und: Wie kann die Immunität des IKRK auch im Netz geltend gemacht werden?

Unbemerkt von der Öffentlichkeit hat sich das IKRK in den vergangenen Jahren als globales Labor für technische Innovationen etabliert. Die Hilfsorganisation, die aktuell unter anderem Kriegsbetroffene in der Ukraine mit lebenswichtigen Gütern versorgt oder im Sudan die Freilassung von Kriegsgefangenen vermittelt, experimentiert in der digitalen Welt mit neuen Technologien. Sie entwickelt zusammen mit Wissenschaftlerinnen Prototypen – zum Beispiel, um Daten unter humanitären Schutz zu stellen- – oder sucht nach Antworten darauf, wie digitale Souveränität nicht nur ein utopisches Konzept bleibt.

Mit anderen Worten: Das IKRK, gegründet 1863 als Reaktion auf die Gräuel in der Schlacht von Solferino, erfindet sich digital gerade neu. Allerdings tut es das nicht in der Schweiz, nicht am Gründungsort und Hauptsitz in Genf, sondern in Luxemburg.

Dort will die Organisation eine sogenannte Cyberdelegation aufbauen, wie sie im November 2022 ankündigte. Jetzt, nur acht Monate später, ist der technische Ableger startklar für Forschungsexperimente – in den hochsicheren Datenzentren Luxemburgs, die diplomatischen Schutz geniessen.

Dies ist die Geschichte, wie sich eine 160 Jahre alte Institution neu erfinden muss, um ihre altbewährten Werte wie Neutralität und Unparteilichkeit in den Cyberspace zu retten. Und wie es die Schweiz verpasste, Standort der Neuerfindung ihres humanitären Aushängeschilds zu werden.

Ein Cyberangriff auf das Internationale Rote Kreuz

Das Hauptquartier des Internationalen Roten Kreuzes thront an der Avenue de la Paix in Genf auf einem kleinen Hügel, 500 Meter vom Schweizer Sitz der Uno entfernt. In Gehdistanz befinden sich ausserdem die russische und noch etwas weiter die ukrainische UN-Mission, die im Genfer Quartier des Nations friedlich nebeneinander koexistieren.

Die strikte Unparteilichkeit ermöglicht es dem IKRK, über die Frontlinien hinweg tätig zu sein, seine humanitäre Arbeit leitet sich, gestützt auf die Genfer Konvention, aus dem Völkerrecht ab. Ob nun gegenwärtig in der Ukraine, in Afghanistan oder im Sudan: Verwundete oder Kriegsgefangene, egal von welcher Konfliktpartei, werden versorgt, die Konvois und das Personal des IKRK nicht angegriffen, seine Hilfsgüter nicht angetastet, seine Legitimität nicht hinterfragt.

Doch im Cyberspace ist all das nichts wert.

Auf den Kriegsschauplätzen im Netz werden die Prinzipien des Völkerrechts täglich gebrochen. Die Zivilbevölkerung und die nicht-militärische Infrastruktur angegriffen. Die Daten von Bürgerinnen geplündert. Nach Angriffsmöglichkeiten in IT-Systemen von Spitälern oder Wasserversorgern gesucht. Desinformationskampagnen auf Tiktok, Instagram oder Twitter fabriziert.

Und dabei geraten auch humanitäre Organisationen ins Visier, wie etwa im November 2021, als bei der bisher grössten Cyberattacke gegen das IKRK 515'000 Personendaten gestohlen wurden.

In der betroffenen Datenbank waren sensible Informationen über Aufenthaltsorte von Personen gespeichert, die wegen Gewalt und Krieg in ihrer Heimat oder aufgrund einer Naturkatastrophe in Not geraten waren. Es handelt sich um Daten von geflüchteten Afghaninnen oder Einwohnern des Inselstaats Tonga, die wegen Überschwemmungen nach einem Tsuna-

mi fliehen mussten. Manche von ihnen gelten als besonders verwundbar, darunter minderjährige Jugendliche.

«Mit dem Angriff auf das IKRK wurde ausgerechnet eine Organisation getroffen, die bereits viel in ihre Cyberabwehr investiert hatte», sagt Charlotte Lindsey vom Cyberpeace Institute der Republik. Die Stiftung, die ebenfalls im Quartier des Nations in Genf residiert, hat sich auf digitale Schutzvorkehrungen für Non-Profit-Organisationen spezialisiert.

Ihre Zahlen für die Schweiz sind alarmierend: Nur 21 Prozent der Schweizer NGO machen vollständige Backups ihrer Daten oder verwenden die 2-Faktor-Authentifizierung für die sichere Anmeldung auf ihren Systemen – etwas, das heute allgemeiner Standard ist.

Im Vergleich dazu ist das IKRK geradezu digitale Avantgarde. Bereits 2010 hatte die Hilfsorganisation den Posten eines Chief Information Security Officer geschaffen. Trotzdem trat der Worst Case ein. «Wir wussten, dass wir eines Tages ein Ziel sein könnten», sagt Balthasar Stähelin, Direktor für Digitale Transformation beim IKRK, gegenüber der Republik. Die Hilfsorganisation hatte ihre Cyberabwehr auf digitale Lieferketten ausgerichtet und überprüfte eingekaufte Softwarekomponenten. Doch den Hack von 2021 konnte sie damit nicht verhindern, denn er war von langer Hand vorbereitet und genau zugeschnitten auf die Server des IT-Dienstleisters des IKRK.

Wer hinter dem Angriff steht, ist bis heute nicht öffentlich bekannt. Das IKRK verfügt über Hinweise auf die Täter, wie mehrere Quellen bestätigen. Doch das Rote Kreuz bleibt auch in diesem Fall neutral. Und macht keine «Attribution», was im Diplomaten- und Techsprech bedeutet: keine öffentliche Schuldzuweisung. Davon abgesehen hat sich das IKRK jedoch für ein unkonventionelles Vorgehen entschieden und kommuniziert schonungslos offen über den Datendiebstahl.

Daten sind Menschenleben

Massimo Marelli arbeitet – mit Unterbrüchen – schon seit 14 Jahren für das Rote Kreuz. Eingestiegen ist der Jurist 2009 mit einem Einsatz als Delegierter im Sudan. Später war er als oberster Datenschützer des IKRK tätig, heute leitet er die neue Cyberspace-Delegation. Er empfängt die Republik an einem warmen Frühlingsnachmittag in einem modischen blauen Anzug in seinem neuen Büro in Luxemburg.

In seinen Bücherregalen stehen in ordentlicher Reihe unzählige Handbücher zur digitalen Transformation des IKRK, die er mitverfasst hat. Während des Gesprächs zückt er immer wieder mal eines. Der gebürtige Italiener reagiert erstaunt auf die Frage, weshalb sich seine Organisation nach dem Hack dafür entschieden hat, in die Offensive zu gehen: «Wir hatten doch keine Wahl.»

«Das IKRK setzt sich gemäss seines völkerrechtlichen Mandats für den Schutz und die Unterstützung der Opfer von bewaffneten Konflikten ein und ist daher auch im Besitz von deren Daten», sagt er. «Wer sein Leben in einer Notsituation dem IKRK anvertraut, muss deshalb auch in der digitalen Welt geschützt werden.» Oder eben offen und transparent informiert. Nicht erst seit der Cyberattacke vertritt Marelli die Formel: «Digital gleich offline.» Damit meint er: Die Daten eines Hilfswerks sind gleichbedeutend mit Menschenleben.

Tatsächlich haben beim IKRK gespeicherte Daten bereits heute denselben rechtlichen Status wie das Personal: Sie geniessen Immunität. IKRK-Mitarbeiter dürfen von einem internationalen Tribunal nicht als Zeuginnen zur Aufklärung von Kriegsverbrechen aufgeboten werden. Für gespeicherte Daten gilt: Sie dürfen vor Gericht nicht verwendet werden.

Doch wie ist der besondere Schutz dieser Daten tatsächlich zu gewährleisten?

Bereits Mitte der 2010er-Jahre überlegte sich das Internationale Rote Kreuz, was nötig sei, um die bewährte humanitäre Mission auch im Netz unabhängig und neutral erfüllen zu können. Es fokussierte sich auf die Resilienz gegen Cyberattacken wie auch auf die Frage, wie sich Abhängigkeiten von ausländischen IT-Unternehmen verringern lassen.

Denn Angriffe von Hackerinnen sind nicht das einzige Problem für das IKRK.

«Nicht angreifen!» als digitales Emblem

Wenn europäische Unternehmen und Behörden Software aus den USA nutzen, hängen amerikanische Überwachungsgesetze über ihnen wie ein Damoklesschwert. Niemand ist vor dem Datenhunger der US-Geheimdienste und Strafverfolgungsbehörden gefeit. Niemand kann hundertprozentigen Schutz vor staatlichen Zugriffen garantieren. Das IKRK hat hier wenig rechtlichen Spielraum. Schnell mal Dokumente auf Google-Drive ablegen oder Nachrichten via Facebook-Messenger versenden? Zu heikel.

«Für den Schutz unserer Datenbanken müssen wir eine spezifische IT-Architektur entwickeln. Wir brauchen aber auch gute Gesetze», sagt Marelli. Anders ausgedrückt: Das IKRK braucht auch in der digitalen Welt echte Immunität.

Der Hackerangriff von 2021 wirkte kurz demoralisierend auf das IKRK. Doch er bestärkte die Organisation in ihrer eingeschlagenen Strategie. 2022 wurde deshalb ein Projekt forciert, das schon lange in der Pipeline steckte: die Schaffung eines digitalen Emblems zum humanitären Schutz von Daten. Es soll Server und Datenzentren von humanitären Organisationen spezifisch kennzeichnen.

Das Signal an Kriegsparteien im Netz wäre dasselbe wie jenes des Roten Kreuzes auf Ambulanzfahrzeugen oder Spitälern in Kriegsgebieten: Nicht angreifen! «Ähnlich wie beim Grundsatz, dass das IKRK Camps niemals in der Nähe von Militärstützpunkten aufbaut, müssen wir uns jetzt überlegen: Wie setzen wir so etwas im Cyberspace um?», sagt Marelli. «Wie signalisieren wir potenziellen Angreifern, dass das, was sie ins Visier nehmen wollen, geschützt ist?»

Doch locken die markierten Server nicht erst recht Angreifer an?

Der IKRK-Cyberdelegierte Marelli hört diese Frage nicht zum ersten Mal. Er findet: Gerade deshalb müsse das Emblemkonzept in allen Varianten simuliert und getestet werden, um Erfahrungen zu sammeln. Und diese Tests für ein digitales IKRK-Update werden nun in zwei geschützten Datenzentren stattfinden, die in Bissen und in Bettemburg in Luxemburg stehen.

Doch warum eigentlich Luxemburg?

Mauern, Bastionen, gesicherte Gewölbe: Luxemburg ist eine Festungsstadt. Überall altes Gestein, das noch aus der Zeit der Verteidigung gegen europäi-

sche Grossmächte stammt. Die Hauptstadt des Grossherzogtums besteht aus einer eleganten Oberstadt auf Hügeln und einer eher dörflich geprägten Unterstadt im Tal, umsäumt von Parks und Wäldern. Das Bild der «Festung Luxemburg» sei eine beliebte politische Erzählung des Landes, sagt Laurent Schmit, stellvertretender Chefredaktor von «Reporter.lu», einem Online-Magazin, das auch auf Deutsch erscheint. Die Republik trifft Schmit an einem sonnigen Vormittag im hippen Café Konrad in der Haute Ville.

Luxemburgische Politikerinnen übertragen die Festungsmetapher gerne auf andere Bereiche, sagt der Journalist: auf die Finanzindustrie als «sicheren Hort des Geldes», auf den Cyberspace als «sicheren Hort der Daten».

Schmit erklärt, die Digitalstrategie seines Landes bestehe zum einen in der Ansiedlung ausländischer Konzerne von Rang und Namen, etwa mit einer attraktiven Steuerpolitik. Amazon zum Beispiel hat im Kleinstaat seinen Europa-Hauptsitz. Ebenfalls in Luxemburg befindet sich der Holdingsitz der israelischen NSO Group, die umstrittene Spyware-Produkte an Regierungen verkaufte.

Zum anderen, sagt Schmit, leiste sich Luxemburg seit Jahrzehnten eine teils eigene digitale Souveränität, indem das Land in hochsichere IT-Infrastruktur in staatlichem Besitz investiert habe. Eine ähnliche Strategie schlug der Staat bereits vor über 45 Jahren ein, als Satelliten aufkamen. Heute gilt die luxemburgische Firma SES als einer der weltweit führenden Satellitenbetreiber. Sie stellt der Nato Kapazitäten für die Abwehr des russischen Angriffskriegs in der Ukraine zur Verfügung.

Das Staats-Backup

2006 liess die luxemburgische Regierung das Unternehmen Luxconnect bauen, das heute vollständig im Besitz der öffentlichen Hand ist. Ursprünglich waren dessen Datenzentren für eine sichere Banken-Cloud gedacht. Doch mit der Einführung des automatischen Informationsaustauschs und strengerer internationaler Regeln hätten einige Banken ihre Geschäftsmodelle reformieren müssen, sagt Schmit. Das warf die Frage auf: Wie lassen sich die supersicheren, aber auch wahnsinnig teuren Rechenzentren sonst noch nutzen?

Die bis heute amtierende Koalitionsregierung, bestehend aus Grünen, Sozialdemokratinnen und Liberalen, lancierte darauf eine Diversifikationsstrategie, liess nach neuen Branchen für die Auslastung der staatlichen Server suchen – und landete 2015 mit dem digitalen Staats-Backup einen diplomatischen Coup.

Die Idee dahinter: Luxemburg bietet Server für die sichere Speicherung von Bürgerinnendaten anderer Länder. Der erste Kunde hiess Estland und war ein idealer Testkandidat. Das baltische Land ist nicht nur *der* europäische Vorzeigestaat in Sachen Digitalisierung, sondern weiss auch, was es bedeutet, ins Visier von Hackerinnen zu geraten.

2007 wurde Estland Ziel einer gigantischen Cyberattacke, die mehrere Wochen dauerte und Ministerien, Banken und Medien betraf. Estland vermutete die russische Regierung hinter dem Angriff, Sicherheitsexpertinnen verdächtigten hingegen private Akteure aus Russland. Unabhängig davon, wer tatsächlich die Täter waren, lautete eine der wichtigsten Erkenntnisse aus dem Vorfall: Die Daten der estnischen Bürgerinnen brauchen in Zukunft ein Backup ausserhalb der Staatsgrenzen, damit Estland bei einem nächsten Angriff funktionsfähig bleibt.

Luxemburg griff diese Idee auf. Und entwickelte das Konzept E-Embassy.

E-Embassy bestehe aus zwei Elementen, erklärt Dejvid Adrović vom luxemburgischen Aussenministerium auf Anfrage: zum einen aus den Services eines hoch sicheren und leistungsfähigen Datenzentrums. Die estnischen Bürgerdaten etwa seien in den Zentren von Luxconnect untergebracht. Das zweite Element: die rechtlichen Privilegien der Datenzentren, die den Status einer diplomatischen Botschaft haben. Das bedeutet: Hier gelten weder EU-Gesetze noch luxemburgisches Recht. Luxemburger Behörden dürfen diese Datenzentren nicht betreten, die Lizenzen und Leitungen gelten als unantastbar.

Das IKRK wurde früh auf das E-Embassy-Konzept Luxemburgs aufmerksam. «Genau nach so was hatte ich gesucht: hoch sichere Datenzentren und diplomatischen Schutz», erinnert sich der IKRK-Cyberdelegierte Marelli. Er nahm Kontakt mit dem Aussen- und Entwicklungsministerium auf und schwärmt auch heute noch: «Luxemburg war eines der ersten Länder, das sich mit den geopolitischen Dimensionen eines Cyber-Gastlands auseinandersetzte und Innovationen in dem Bereich förderte.»

Nach dem Cyberangriff auf das IKRK ging es plötzlich schnell.

Im September 2022 zog Marelli mit seiner Cyberdelegation an die Rue Jean-Pierre Brasseur 1 in einem der oberen Stockwerke ein, die Adresse befindet sich in einem ruhigen Aussenquartier der Luxemburger Hauptstadt. Das Gebäude teilt sich die IKRK-Delegation mit Anwälten und Finanzfonds. Das Luxemburger Team ist noch klein, und umfasst elf Mitarbeiterinnen. Diese sollen Lösungen entwickeln, die später im besten Fall in den «Normalbetrieb» des IKRK überführt werden, die dann von «klassischen» Delegationen genutzt werden können. Die Testumgebung bei Luxconnect ist inzwischen eingerichtet.

Am 13. Juli dieses Jahres hat Luxemburgs Parlament als Legislative des digitalen Gaststaates das sogenannte Sitzabkommen mit dem IKRK fast einstimmig ratifiziert und damit die Ansiedlung der IKRK-Cyberdelegation offiziell vollzogen.

Und was ist mit Genf?

Genf steht als Sitz humanitärer Organisationen in einem harten Standortwettbewerb mit anderen europäischen Städten. Das ist in der Genfer NGO-Szene ein offenes Geheimnis. Eine Insiderin, die lange beim IKRK arbeitete, sagt: «Wir haben früher schon mit Genf und Bern Gespräche geführt über unsere Bedürfnisse zur digitalen Immunität und signalisiert, dass wir mit anderen Staaten im Gespräch sind.» Doch richtig ernst genommen habe das die Schweiz nicht.

Die offizielle Version des Cyberdelegierten Massimo Marelli ist eine andere: Das IKRK ging zuerst auf Luxemburg zu. Einfach weil das Angebot schon da war. Und egal, mit wem man spricht: Die IKRK-Verantwortlichen wollen den Ableger in Luxemburg explizit nicht als Abkehr von Genf verstanden wissen. «Wir sind der Schweiz in jeglicher Hinsicht sehr verbunden und arbeiten eng mit den Behörden und der Wissenschaft zusammen», betont Marelli immer wieder. Auf dem Beistelltisch liegt mitgebrachte Schokolade der Genfer Marke Favarger.

Es stimmt: Die Denkarbeit zu digitalen Innovationen findet nach wie vor auch in der Schweiz statt. So hat die Eidgenössische Technische Hochschule Lausanne (EPFL) kürzlich ein Papier veröffentlicht, wie das

IKRK Biometriedaten von geflüchteten Personen mit möglichst niedrigem Missbrauchspotenzial speichern könnte. Fingerabdrücke oder Gesichtsbilder gehören zu den sensibelsten Informationen einer Person, sie vereinfachen aber auch die durchgängige Identifizierung von Geflüchteten. Das IKRK hat deshalb mit EPFL-Forschern wie der renommierten Professorin und Privacy-Expertin Carmela Troncoso ein Konzept für eine dezentrale Lösung auf Smartphones entwickelt, um den Bau von zentralisierten Datenbanken zu vermeiden.

Der Trend des IT-Outsourcing ist jedoch nicht schönzureden: Die digitale Transformation der in Genf ansässigen internationalen Organisationen findet überall statt – nur nicht in der Schweiz. Etliche Institutionen haben ihre technischen Ableger bereits woanders aufgebaut. Etwa das UNICC, der technische Dienstleister der Uno, der ein grosses Datenzentrum in Valencia aufbaut. Oder die WHO, die einen «Hub for Pandemic and Epidemic Intelligence» in Berlin entwickelt.

Warum diese Entwicklung? Hat Bern geschlafen? Verliert das internationale Genf den digitalen Anschluss?

Im Bundesparlament scheint man noch nichts vom Luxemburger IKRK-Ableger mitbekommen zu haben. Franz Grüter, Präsident der aussenpolitischen Kommission im Nationalrat und SVP-Nationalrat, hat sich zwar mehrfach zu den aktuellen Sparmassnahmen beim IKRK geäussert. Von der Cyberdelegation der humanitären Delegation hört er von der Republik aber zum ersten Mal. Und er findet, wie er auf Anfrage sagt, auch das Konzept der E-Embassy «durchaus interessant».

Streng genommen bietet die Schweiz den internationalen Organisationen dieselben rechtlichen Rahmenbedingungen wie Luxemburg: digitale und reale Unversehrtheit. Zwar hat das IKRK in der Schweiz keinen Botschaftsstatus, aber die Gebäude, der Boden, die Infrastruktur des IKRK sowie auch ihre IT-Dienstleister, die über Daten des Roten Kreuzes verfügen, stehen unter dem «Gebot der Unverletzlichkeit».

«Schweizer Behörden sind verpflichtet, jede Form der Durchsuchung, Beschlagnahmung (...) oder jeder anderen Form von exekutivem, administrativem, gerichtlichem oder gesetzgeberischem Zwang zu unterlassen», schreibt dazu das Aussendepartement auf Anfrage der Republik. Die Schweizer Justiz habe ausserdem keine Befugnisse, einem allfälligen Rechtshilfegesuch zum Beispiel der USA nachzukommen und vom IKRK eine Datenherausgabe zu erzwingen.

Macht Luxemburg also einfach besseres Marketing? Nicht nur.

Einerseits bietet der Kleinstaat mit Luxconnect eine hoch sichere und leistungsfähige Infrastruktur, die hierzulande fehlt. Andererseits wird die von der Schweiz gewährte Unverletzbarkeit des IKRK zwar in allen Bereichen durchgesetzt – ausser bei der Cybersecurity. Im Strategiepapier «Digitalaussenpolitik 2021–2024» sind weder Schwerpunkte noch Aktionspläne dazu festgehalten. Zwar wollte das Aussendepartment darin das internationale Genf als Hort der internationalen Digitalpolitik positionieren. Doch es fehlte an einer Vision, wie die humanitären Organisationen selbst als digitale Labors fungieren könnten.

Dies scheint sich nun zu ändern.

Der Cyberangriff auf das IKRK war immerhin ein Weckruf für Genf und Bern. Eine Erinnerung daran, dass Regeln allein nicht ausreichen. In der jüngst verabschiedeten NCS-Cybersecurity-Strategie des Bundes finden die

internationalen Organisationen in der Schweiz erstmals explizit Erwähnung. So steht unter dem Punkt «Stärkung des digitalen internationalen Genfs», die Schweiz müsse prüfen, welche Rahmenbedingungen es brauche, damit sich «diese Organisationen vor Cyberdrohungen schützen können».

«Die Cyberresilienz im humanitären Sektor» müsse erhöht werden, sagt dazu auch Katharina Frey Bossoni, die stellvertretende Leiterin der Abteilung Digitalisierung im Aussendepartement: «Wir arbeiten daran, auch ein digitaler Gaststaat zu werden.» Gegenwärtig werde das Sicherheitsdispositiv in dieser Hinsicht weiterentwickelt.

Offenbar machen sich auch hochrangige Kader des Aussenministeriums in dieser Sache kundig: Im Juni 2023 flog eine Delegation unter der Leitung des Botschafters und Digitalisierungschefs Benedikt Wechsler nach Washington um sich mit Kollegen vor Ort über Fragen zur Cyber- und Digitaldiplomatie auszutauschen.

Und nicht zuletzt soll die Swiss Government Cloud des Bundesamts für Informatik und Telekommunikation, die sich im Aufbau befindet, dem IKRK zur Verfügung stehen, wie aus einer Republik-Recherche hervorgeht.

Diese Fortschritte sind dringend nötig. Denn die Datenbanken mit allen IKRK-Personendaten stehen weiterhin in der Schweiz. Vorerst.