

Israel: „Silicon Wadi“ – nein, es handelt sich bei dieser Wortzusammensetzung nicht um einen Schreibfehler, sondern um die hebräische Übersetzung für Silicon Valley. Silicon Wadi ist das israelische Gegenstück zum Innovationsstandort im US-amerikanischen Kalifornien und konzentriert sich räumlich in Tel Aviv und Umgebung. Der Großteil, über siebzig Prozent, aller israelischen Start-ups ist hier ansässig.

In Israel, ähnlich wie im Ausland, wird das kleine Land, das in etwa die Fläche des Bundeslandes Hessen umfasst und knapp neun Millionen Einwohner zählt, mit seinen rund 6.000 Start-ups häufig als *„Start-up-Nation“* des Nahen Ostens gefeiert. Kennzahlen zufolge ist Israel neben China und den USA einer der beliebtesten Standorte für Investitionen in Start-ups weltweit. Eine Branche floriert besonders: die Cyberabwehr und -sicherheit, die 450 Unternehmen zu ihrem Geschäft gemacht haben. In diesem Start-up-Zweig hat Israel China 2018 überholt, nachdem größeres ausländisches Wagniskapital in das nahöstliche Land als in den fernöstlichen „Riesen“ gepumpt worden war. Nahezu zwanzig Prozent des globalen Wagniskapitals flossen im vergangenen Jahr nach Israel. Nur die USA ziehen bislang mehr Investoren in dieser Branche an.

Wie hat ein flächenmäßig so kleines und bevölkerungsarmes Land wie Israel es geschafft, eine der innovativsten Nationen im Bereich der Cyberabwehr und Cybersicherheit zu werden? Eine Antwort auf diese Frage gibt ein Blick in die Geschichte des jungen Landes. Die Freude über die Staatsgründung 1948 hielt nicht lange an, nachdem das gerade aus der Taufe gehobene Land nach der Ausrufung der Unabhängigkeit von seinen arabischen Nachbarstaaten angegriffen worden war. Abgesehen von Waffenlieferungen aus der damaligen Tschechoslowakei und Frankreich erhielt Israel keine nennenswerte Militärhilfe von anderen Staaten. Die Erfahrung, sich im Zweifel nicht auf die Unterstützung anderer Nationen verlassen zu können, wiederholte sich im Zuge des Sechstagekriegs 1967, nachdem Frankreich seinen vormaligen Protegé mit einem Rüstungs-embargo belegt hatte. Aus diesen Ereignissen zog Israel den Schluss, in Forschung und Entwicklung in der Verteidigungsindustrie zu investieren, um sich unabhängiger von Rüstungsmaterial aus dem Ausland zu machen. Israel hat in den zurückliegenden siebzig Jahren neben den zwei erwähnten Kriegen fünf weitere gegen seine arabischen Nachbarn geführt. Folglich misst das Land seinem Rüstungssektor – seit vielen Jahren einschließlich der Cyberkapazitäten – eine sehr große Bedeutung bei.

So überrascht es nicht, dass in Israel wie in kaum einem anderen Land viele Unternehmen im Bereich der Militärtechnik gegründet werden. Neben der historischen Erklärung begünstigt die Wehrpflicht, die für Frauen und Männer gleichermaßen gilt, die enge Verzahnung des Sicherheits- und Verteidigungsapparats mit der Start-up-Landschaft. Gemäß dem „Drehtüreffekt“ gründen viele ehemalige Militärangehörige

Start-ups, die ihrem vorherigen Arbeitgeber Dienstleistungen und Kapazitäten anbieten – schließlich haben Personen, die ihre Uniform gegen Flipflops und Schirmmütze eintauschen, intensive Erfahrungen im israelischen Militärapparat.

Sowohl von staatlichen als auch nicht staatlichen Akteuren gehen im Cyberraum immer häufiger gravierende Gefahren aus; für Streitkräfte ebenso wie für Zivilgesellschaften. Es gibt kaum noch Verteidigungssysteme, die nicht an zentrale Netze angeschlossen sind, was ein hohes Verwundbarkeitspotenzial nach sich zieht.

Israel hat die wachsende Vernetzung zwischen physischer Infrastruktur und der Online-Sphäre und den damit einhergehenden Gefahren, aber auch Chancen im Cyberraum frühzeitig erkannt. Die Eliteeinheit 8200 der *Israel Defense Forces* (IDF) trägt maßgeblich dazu bei, die Cyberinfrastruktur Israels zu der weltweit führenden zu entwickeln. Neben dem Militär ist auch die Regierung erheblich daran beteiligt, Cyberinnovationen im Land anzuschieben. Die Israelische Innovationsbehörde (*Israel Innovation Authority*) ist der größte Cyberinvestor im Land.

Dass in einem solchen Umfeld sehr junge und kleine Unternehmen Aufträge des israelischen Militärs erhalten, ist keine Seltenheit. So wurde kürzlich ein Start-up, das seit 2013 in einem Kibbuz in der Nähe der Grenze zum Gazastreifen ansässig ist und von ehemaligen Angehörigen der Drohnen-Einheit der IDF gegründet wurde, mit der Entwicklung einer Überwachungsdrohne für die israelische Infanterie beauftragt. Zwar tat sich das Start-up mit einem größeren israelischen Unternehmen zusammen, um die IDF-Ausschreibung für sich zu entscheiden. Dennoch ist beachtlich, dass ein Jungunternehmen an der Entwicklung von Militärtechnik beteiligt wird – zumal dann, wenn (staatseigene) Giganten der Branche bei einer solchen Ausschreibung ausgestochen werden.

So selbstverständlich Militär, Regierung und Privatwirtschaft in Israel ineinander greifen, um das Land gegen Cybergefahren zu rüsten, so sehr steht Deutschland noch am Anfang, sich der Probleme auf diesem immer bedeutsameren Gebiet anzunehmen. Erst seit 2017 befindet sich das Kommando Cyber- und Informationsraum der Bundeswehr als eigenständiger militärischer Organisationsbereich im Aufbau. Die rechtlichen und politischen Rahmenbedingungen sind in Deutschland zwar andere – nicht zuletzt aufgrund der 2011 ausgesetzten Wehrpflicht –, dennoch lohnt ein Blick nach Israel, um mögliche Lehren für den eigenen Ausbau der Cyberabwehr aus dem nahöstlichen Erfolgsmodell zu ziehen.

Aylin Matlé
Auslandsbüro Israel der Konrad-Adenauer-Stiftung