Israels Ansatz als Erfolgsmodell


Daniel Heller

Die Widerstandsfähigkeit moderner Gesellschaften gegen Bedrohungen aus dem Cyberbereich – Cybercrime und Cyberwar – ist entscheidend für deren Erfolg im Konzert der Geopolitik. In den vergangenen Jahren wurde Israel zu einem erfolgreichen Zentrum im Bereich Cyber Security und einer 82 Milliarden US-Dollar schweren Cyber-Industrie.

Die zunehmende Vernetzung und neue Formen der Informationsgesellschaft führen laufend zu neuen Formen der Angriffsmöglichkeiten. Deshalb ist die Resilienz, also die Widerstandsfähigkeit, gegenüber den Bedrohungen aus dem Cyber- und Informationsraum entscheidend für die Zukunft moderner Gesellschaften.

Israel macht vor, wie man sich gegen Cyber Risiken wappnet. Die israelische Wirtschaft hat bereits über 300 Cyber-Security-Startups hervorgebracht und ist in internationalen Kooperationen führend. Bereits über 30 multinationale Konzerne haben in Israel lokale Forschungs- und Entwicklungszentren eröffnet. Das Zentrum des israelischen Cyber-Defence-Biotops befindet sich im Advanced Technologies Park an

der Ben-Gurion University in der Stadt Beer-Sheva, wo angewandte Forschungslabore Ihren Sitz haben.

SECHS ERFOLGSFAKTOREN

Die Erfolgsgeschichte Israels lässt sich auf sechs Erfolgsfaktoren zurückführen:

1. **Koordination durch die Behörden:** Anstelle unflexibler Mehrjahrespläne setzt Israel in seiner «National Cyber Initiative» auf die Entwicklung eines responsiven Ökosystems, welches auf unvorhersehbare Bedrohungen reagieren kann. Das System zeichnet sich durch eine kontinuierliche Kooperation von Behörden, Streitkräften, Wirtschaft und Forschung aus.
2. **Behörden als Katalysator:** Das 2011 gegründete «National Cyber Bureau» beförderte Israel innert weniger Jahre unter die fünf führenden Nationen im Bereich Cyber Security. Kombiniert mit der reichen Erfahrung im Forschungs- und Anwendungsbereich, entwickelte sich die Cyber-Industrie zu einem zentralen Wachstumstreiber für Israel.
3. **Streitkräfte als Startup-Förderer:** Die historisch bedingte, überproportionale Ressourcenallokation zur Entwicklung moderner Militärtechnologie agierte als Katalysator für den rasanten Fortschritt im Bereich Cyber Defence. Cyber Defence entwickelte sich zu einer Schlüsselkompetenz des Verteidigungsministeriums, und Cyber-Defence-Einheiten fungieren Start-up ähnlich als wichtiger Treiber der israelischen Wirtschaft.
4. **Aufbau von Humankapital:** Menschen mit ihren Fähigkeiten, Erfahrungen und Ambitionen bilden die Ingredienz für erfolgreiche Cyber Defence. Das israelische Bildungssystem fördert bereits auf Stufe Maturität das Fach Cyber Security bis hin zum PhD.
5. **Interdisziplinarität und Vielfalt:** Cyber Security umfasst juristische, psychologische, soziologische und wirtschaftliche Perspektiven. Israel kombiniert erfolgreich militärische Erfahrungen mit akademischem Know-how, und setzt dieses erfolgreich in der Wirtschaft um.
6. **Fähigkeitsbasierter Ansatz:** Bisherige Cyber-Abwehrstrategien sind meist in Reaktion auf eine unmittelbare Bedrohung entstanden. Über viele Behörden verteilte Kompetenzen solcher Ad-hoc-Strategien machen diese ineffizient, fragmentiert und kaum koordinierbar. Israel hingegen verfolgt den Ansatz einer proaktiven, kohärenten, disziplinenübergreifenden und langfristigen Strategie, welche den Aufbau von Kompetenzen als zentrales Element erachtet.

FAZIT UND FOLGERUNGEN FÜR DIE SCHWEIZ

Eine erfolgreiche, an die Erfahrungen Israels angelehnte, Cyber-Strategie muss auf drei Ebenen ansetzen:

1. **Robustheit:** Immunisierung der Infrastruktur und Netze gegen Attacken. Der Staat berät und führt, während betroffene Organisationen und Unternehmen eigenverantwortlich handeln.
2. **Resilienz:** Schutz vor neuen Risiken dank Erforschung, Aufklärung und Entschärfung von Bedrohungen, unterstützt durch das aktive Engagement staatlicher Experten.
3. **Verteidigung:** Die erfolgreiche Verteidigung erfordert Ressourcen und Kapazitäten, die nur Staaten und ihre Behörden aufbringen können.

Neben guten Ansätzen braucht die Schweiz nun konkrete Umsetzungsschritte,

- mehr Mittel und Ressourcen in diesem Bereich,
- eine bewährte Arbeitsteilung zwischen Staat und Wirtschaft nach den Prinzipien des «Public Private Partnership»,
- eine bewährte Aufgabenteilung zwischen Bund und Kantonen nach den Prinzipien der Subsidiarität und der Wirksamkeit.

Starre Strukturen sind zu beseitigen und durch eine integrative Verteidigungsstrategie zu ersetzen. Es gilt, auf bisherigen analogen Stärken wie Rechtssicherheit und Bildung aufzubauen und diese im digitalen Raum zu adaptieren. Nur so kann der Schutz der Schweiz einerseits, aber auch die langfristige Förderung des Innovations- und Wirtschaftsstandorts andererseits, gewährleistet werden.