Warum Zivilisten beim Cyberwar die Führung übernehmen sollten

Thomas Roithner

Militärische Apparate und Organisationen sind trickreich. Und erfindungsreich. Und manchmal beides gleichzeitig. Das ist auch deshalb höchst beachtenswert, weil man dies – landläufig vorurteilsbehaftet – einem schwerfälligen Apparat kaum zutraut. Die Suche nach Bedrohungen und vor allem die Zuständigkeitserklärung des Militärs für Ziviles blickt auf eine lange Tradition zurück und hat sich in letzter Zeit hierzulande ins beinahe Unberechenbare entwickelt. Die jüngste Debatte um mehr Befugnisse im sogenannten „Cyberwar“ gehört zweifellos dazu.

„Versicherheitlichung“

So erklärt sich die Österreichische Sicherheitsstrategie aus dem Jahr 2013 – auch wenn über unterschiedliche Ministerien hinaus – für verschiedene Themenbereiche als zuständig. Darunter fallen beispielsweise Wirtschaftskriminalität, Drogenhandel, nicht gelingende Integration, Knappheit von Ressourcen, Klimawandel, Umweltschäden und Pandemien oder die sicherheitspolitischen Auswirkungen der internationalen Finanz- und Wirtschaftskrise. Zu diesen Herausforderungen und Bedrohungen gehören auch „Angriffe auf die Sicherheit der IT-Systeme (Cyberattacks)“ sowie „die Bedrohung strategischer Infrastruktur“. In aller Stille werden zivile Herausforderungen „versicherheitlicht“.

Auch wenn man im Heer das Gesamtkonzept und die Zuständigkeit aller Akteure betont, so holt man Aufgaben wie Cybersicherheit, Cyberkriminalität oder den Missbrauch des Internets für extremistische Zwecke gekonnt ins eigene Boot. Und damit natürlich finanzielle Mittel und Legitimität für klassische Militärapparate. Auch wenn zur gesamtstaatlichen Aufgabe erklärt – es „kann zu einem neuen militärischen Aufgabenfeld werden“, so die Sicherheitsstrategie Österreichs. Das permanente öffentliche Betonen dieses Aufgabenbereiches durch das Militär lässt keinen Zweifel am Herrschaftsanspruch.

Geoökonomie

Selbstverständlich sind Angriffe auf IT-Systeme kriminelle Handlungen. Sie brauchen Prävention, Aufklärung, Verfolgung und Justiz. Die globalen ökonomischen Entwicklungen zwischen Staaten und Wirtschaftsräumen (Geoökonomie) sind rauer geworden. Auch für die einzelnen Akteure. Die gleichzeitige Abhängigkeit und Konkurrenz von den USA und China ist nur eines von vielen Beispielen. Geopolitik und Geoökonomie greifen ineinander und dies ist nicht immer stabilitätsfördernd.

Global betrachtet müssen eine nervöse Wirtschaftslage und ein damit oftmals verbundener aggressiver ökonomischer Wettbewerb von nervösen Fingern am Abzug strukturell so weit wie möglich getrennt werden. Zivile Bedrohungen benötigen gut ausgestattete zivile Bearbeitungsmöglichkeiten statt eine Militarisierung.

Staatsstruktureller Cyberfrieden

Ob die Gewährleistung der Cybersicherheit dort man besten aufgehoben ist, wo auch die Waffenarsenale aufgehoben sind, ist in höchstem Maße anzuzweifeln. Auch im innerstaatlichen Verhältnis sind die Strukturen zur Wahrung der Sicherheit der IT-Systeme so auszurichten, dass die Felder Cyberattacks und Kriegsführung so weit wie möglich auseinanderliegen. Eskalationsspiralen und dem Durchbrennen zivilisatorischer Sicherungen kann auf diese Weise besser entgegengewirkt werden. Auf dem Weg von der Polizei zum Militär steht optimaler Weise auch eine gesellschaftliche Debatte. Zur Näherung an einen Cyberfrieden soll das Militär nicht gänzlich ausgeschlossen werden, jedoch von seiner tonangebenden Verantwortung entbunden werden. Weil Polizei und Militär in Demokratien aus guten Gründen getrennt sind.

Zur Person: Thomas Roithner ist Sozial- und Wirtschaftswissenschafter, Friedensforscher und Privatdozent am Institut für Politikwissenschaft der Universität Wien.

Quelle: Roithner Thomas: Warum Zivilisten im Cyberwar die Führung übernehmen sollten, in: Neue Zürcher Zeitung Österreich, nzz.at, https://nzz.at/phenomenon/warum-zivilisten-im-cyberwar-die-fuehrung-uebernehmen-sollten/ (direkt anwählbar mit https://nzz.at/s/m_KvZLx9), 8. Dezember 2015, Wien 2015.