

„Wir werden sicherlich den ein oder anderen an die Privatwirtschaft 'verlieren'“



Georg Kunovjanek ist Oberst des Generalstabdienstes und Leiter des neuen Studienganges (Bildquelle: Theresianische Militärakademie)

An der Theresianischen Militärakademie werden seit vergangenem Herbst auch Offiziere für Informations- und Kommunikationstechnik für das österreichische Bundesheer ausgebildet. Im Interview spricht Oberst Georg Kunovjanek über Inhalte, Einsatzgebiete und warum er sich nicht vor dem Wettbewerb mit der Privatwirtschaft fürchtet.



von Johannes Steger

veröffentlicht am 24.03.2023

Herr Kunovjanek, an der Theresianischen Militärakademie werden seit vergangenem Herbst auch Offiziere für Informations- und Kommunikationstechnik ausgebildet. Verteidigungsministerin Klaudia Tanner will damit auch Bedrohungen wie hybride Konflikte, Cyberangriffe oder einen Einsatz von Drohnen begegnen. Wurde der Studiengang also vor dem Hintergrund einer neuen Bedrohungslage begründet?

Es gab unterschiedliche Antriebsfedern, die dazu geführt haben, diesen Studiengang zu etablieren. Einerseits, und das ist das Offensichtlichste, haben wir begonnen, ein neues Kommunikationssystem in der Truppe einzuführen. Es braucht hierfür das Spezialwissen, diese Netzwerkkonstrukturen entsprechend zu konfigurieren, zu überwachen und in Betrieb zu halten. Das war der ausschlaggebende Grund, warum man überlegt hat, neben den klassischen Offizieren für die Landstreitkräfte auch IKT-Offiziere auszubilden. Aber natürlich sind es auch Antriebe wie die derzeitige Sicherheitslage, die durch den Krieg in der Ukraine noch einmal verschärft wurde – auch in Bezug auf die erwähnten hybriden Risiken.

Es war beim Amtsantritt unserer Ministerin immer ihr Credo, auch in diesem Bereich die entsprechenden Ressourcen freizumachen, um einerseits im Militär einen gewissen Eigenschutz sicherzustellen, aber andererseits als Bundesheer Assistenz für andere Ministerien zu ermöglichen. Das ist der zweite Strang der Motivation, diesen Studiengang zu etablieren.

Wir bilden hier aber keine Cyberspezialisten aus. Es sind Offiziere, die eine starke Affinität für diesen Bereich haben, die quasi als Übersetzer zwischen Militär und Technik fungieren, sich in beiden Welten bewegen können. Wir legen hier die Basis für die entsprechende Spezialisierung – und die kann dann später vom klassischen Kommunikationswesen bis hin zur elektronischen Kampfführung reichen.

Sprechen wir hier auch von aktiver Cyberabwehr?

Wir vermitteln unseren Studierenden ebenfalls Wissen in diesem Bereich – aber vor allem über die gesetzlichen Rahmenbedingungen, in denen sich militärisches Handeln immer bewegen muss. Wir beschäftigen uns mit der Debatte, die wir gesamtgesellschaftlich führen: Wie kann der Staat nicht-staatliche Kritische Infrastruktur schützen, welche Kompetenzen müssen dafür beim Staat, welche in der Wirtschaft aufgebaut werden? Liegt die Verantwortung für die Abwehr bei der Polizei oder wirklich beim Militär? Die Deutungshoheit darüber liegt in Österreich beim Innenressort und das Militär hat sich auf die Kompetenz des militärischen Eigenschutzes zu konzentrieren.

Welche Inhalte werden sonst vermittelt?

Es ist im Prinzip ein militärisches Grundlagenstudium, ein weiterer zentraler Aspekt sind die IKT-Grundlagen, also etwa Programmierung von verschiedenen Webtechnologien und Datenbanken, das Training in Cyberranges bis hin zur Wissensvermittlung über unterschiedliche Kommunikations-Technologien. Am Ende soll dann die Spezialisierung erfolgen, also etwa für die IKT-Truppe, die Elektronische Kampfführung oder den Cyber-Bereich.

Sorgen Sie sich nicht, dass Sie hier Topkräfte ausbilden, die dann am Ende in die gut bezahlten Jobs in die Privatwirtschaft wechseln?

Wir werden sicherlich den ein oder anderen an die Privatwirtschaft „verlieren“. Aber ist das wirklich schlimm? Ich denke nicht, denn gesamtstaatlich betrachtet kann es nur ein Gewinn sein, wenn beispielsweise so jemand bei einem Energieversorger für die Cybersicherheit zuständig ist. Wenn ich auf unsere erste Kohorte an Studierenden schaue, dann bin ich sehr zuversichtlich, dass sie sowohl für das Militär als auch die Wirtschaft ein großer Gewinn wären – aber eben auch die dienstlichen Möglichkeiten zur Entwicklung erkennen.

Sie sprachen Eingangs von Assistenzleistungen für andere Ministerien – wie sähe so etwas aus?

2020 wurde das Außenministerium Ziel einer schwerwiegenden Cyberattacke – wir als Bundesheer konnte damals bei der Abwehr und Sicherstellung der Arbeitsfähigkeit unterstützen.

2021 wurde der deutsche Landkreis Anhalt-Bitterfeld Ziel einer Cyberattacke – die Bundeswehr musste Amtshilfe leisten. Das war in Deutschland mitunter umstritten – wird der Einsatz des Bundesheeres im Inland anders gesehen?

Das ist, wenn Sie so wollen, ein sehr österreichisches Spezifikum. Das was in Deutschland etwa das Technische Hilfswerk leistet, ist hierzulande oftmals die Aufgabe des Bundesheeres. Wir haben eine sehr lange Tradition, was Assistenzleistungen im Inneren betrifft. Das wurde noch verstärkt im Zuge des Zusammenbruchs des Warschauer Paktes.

Das Ende des Kalten Krieges an unserer Ostgrenze, wo wir so die Kräfte vor allem des Zolls, aber dann später auch der Polizei unterstützt haben, in der Grenzraumüberwachung, also klassische polizeiliche Aufgaben. Wir sind es daher gewohnt, in dieser der Polizei nachgeordneten Rolle zu agieren und die Öffentlichkeit hat sich daran gewöhnt, dass Soldaten mit der rot weiß roten Schleife im Inland zum Einsatz kommen.

Im Zuge des bereits erwähnten Angriffs auf das Außenministerium handelte es sich allerdings um eine sehr „klassische“ Situation des Einsatzes – also eine Form von Landesverteidigung.

Die Fragen stellte Johannes Steger