presse

Wir brauchen mehr Personal für die Cybersicherheit

***Lars Klingbeil**, netzpolitischer Sprecher;*
***Rainer Arnold**, verteidigungspolitischer Sprecher:*

Eine Bündelung der IT-Kompetenzen und eine Stärkung der Cybersicherheit wie sie Bundesverteidigungsministerin von der Leyen am Donnerstag angekündigt hat, sind angesichts der Herausforderungen durch die Cyberangriffe dringend geboten. Dafür braucht es vor allem mehr Personal bei der Bundeswehr.

„Es ist richtig, dass Frau von der Leyen die Strukturen der Bundeswehr endlich an die digitalen Realitäten anpassen will. Die zivile und militärische Informationstechnik ist der größte Querschnittsbereich in der Bundeswehr mit einem Gesamtvolumen von über einer Milliarde Euro im Jahr. Die Bundeswehr muss auf die veränderten Bedrohungsszenarien reagieren und die Strukturen im Bereich der Cyber-IT grundlegend verändern.

Es ist gut, dass die Ministerin den Bereich der Cyberpolitik eigenständig aufstellt. Die Bündelung zu einem neu aufzustellenden, eigenen Kommando in der Bundeswehr allein wird aber nicht ausreichen, um den Anforderungen der Cybersicherheit gerecht zu werden. Wir begrüßen deshalb ausdrücklich, dass die Ministerin die Entscheidung ihres Amtsvorgängers, den IT-Bereich dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung (BAAINBw) in Koblenz zu unterstellen, wieder rückgängig macht.

Die größte Herausforderung sehen wir darin, ausreichend qualifiziertes Personal für den IT- Bereich gewinnen zu können. Das geht nur, wenn zusammen mit dem Innenministerium eine Initiative entwickelt wird. Nicht nur die Bundeswehr, der gesamte öffentliche Dienst muss attraktiver werden für Cyber-Spezialisten. Dafür müssen entsprechende Mittel im Haushalt bereitgestellt werden.

Die Stärkung und der Ausbau der Cyber-IT sind auch wichtig, um den Herausforderungen durch Cyberangriffe zu begegnen. Die Stuxnet-Schadsoftware war erst der Anfang dieser Entwicklung. Inzwischen gibt es

beinahe täglich Berichte über Cyberangriffe, Kompromittierung, Ausspähung, Manipulation oder Sabotage von IT-Systemen und kritischen Infrastrukturen.

Dieses neue Gefährdungspotenzial ist keine Modeerscheinung, sondern wird die Sicherheits- und Verteidigungspolitik dauerhaft verändern. Wir wollen eine offene Debatte darüber, ob und in welchem Umfang die Bundeswehr digitale Offensivfähigkeiten benötigt. Gleichzeitig muss sich die Bundesregierung stärker als bisher für internationale Vereinbarungen im Bereich der Cybersicherheit einsetzen. Dazu gehören auch Überlegungen zur Anpassung des Völkerrechts an die digitale Wirklichkeit im Sinne eines Völkerrecht des Netzes.“