Cybersicherheit: Wissens-, Kompetenz- und Vollzugsdefizite

(idw) Cybersicherheit: Wissens-, Kompetenz- und Vollzugsdefizite

#8222;Neue Ph
#228;nomene wie Cyberkriminalit
#228;t, Cyberspionage und Cybersabotage sind in den vergangenen Jahren zu ernsthaften Bedrohungen f
#252;r Wirtschaft, Politik und staatliche Infrastrukturen geworden
#8220;, sagt Jakob Kullik von der Professur Internationale Politik der Technischen Universit
#228;t Chemnitz. Unter Cyberkriminalit
#228;t fallen das massenhafte Hacken von E-Mail-Accounts und der Diebstahl von digitalen Identit
#228;ten. Cyberspionage bezeichnet beispielsweise das Vorgehen des US-amerikanischen Auslandsgeheimdienstes NSA, der systematisch und weltweit digitalen Datenverkehr
#252;berwacht. Cybersabotage liegt unter anderem vor, wenn Hacker die Kan
#228;le von Medien knacken und gezielt Falschmeldungen lancieren. Der Chemnitzer Politikwissenschaftler Jakob Kullik ging von Ende 2012 bis Ende 2013 der Frage nach: Besitzt Deutschland eine eigene konsistente Cybersicherheitspolitik? Die Ergebnisse seiner Untersuchung sind als Buch erschienen und bilden unter dem Titel
#8222;Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik
#8220; den Band 7 der
#8222;Chemnitzer Schriften zur europ
#228;ischen und internationalen Politik
#8220;. Kullik untersuchte den strategischen Ansatz, die politisch-institutionelle Struktur, die staatlichen IT-F
#228;higkeiten und den rechtlichen Rahmen. Als methodische Grundlage verwendete er die qualitative Politikfeldanalyse.
#8222;Abschlie
#223;end kann festgehalten werden, dass Deutschland eine eigene Cybersicherheitspolitik besitzt, diese jedoch auf vielen Feldern nicht konsistent ist
#8220;, fasst Kullik seine Ergebnisse zusammen und erkl
#228;rt:
#8222;Neben bestehenden rechtlichen L
#252;cken und Graubereichen existieren in den Reihen der staatlichen Legislative und Exekutive nach wie vor ernsthafte Wissens-, Kompetenz- und Vollzugsdefizite.
#8220;

14 der 28 Mitgliedsstaaten der Europ
#228;ischen Union besitzen derzeit eine nationale Cybersicherheitsstrategie, so die politikwissenschaftliche Studie. Deutschland geh
#246;re innerhalb der EU zu den f
#252;nf f
#252;hrenden Mitgliedsstaaten mit einer eigenen Cyberpolitik. Im Februar 2011 hat die Bundesregierung ihre erste, ressort
#252;bergreifende Cybersicherheitsstrategie verabschiedet, die zentrale Ma
#223;nahmen zur Verbesserung der nationalen Cybersicherheit enth
#228;lt.
#8222;Seither steht das Thema Cybersicherheit weit oben auf der sicherheitspolitischen Agenda der Bundesregierung
#8220;, so Kullik. Die Milit
#228;rs und Geheimdienste der USA, Chinas und Russlands h
#228;tten jedoch bereits in den 1990er-Jahren begonnen, konzeptionelle Strategien f
#252;r milit
#228;rische Operationen im Cyberspace auszuarbeiten. Und Deutschlands Konkurrenten seien nicht nur bekannte Akteure, wie die Volksrepublik China und die Russische F
#246;deration, sondern auch die USA und Gro
#223;britannien.
#8222;Trotz des zu erwartenden Anstiegs von Cyberkriminalit
#228;t in den n
#228;chsten Jahren ist das Risiko- und Gefahrenbewusstsein f
#252;r diese neue Bedrohungsform innerhalb der Gesellschaft nach wie vor gering ausgepr
#228;gt
#8220;, sch
#228;tzt Kullik ein und erl
#228;utert:
#8222;Eines der Hauptprobleme ist, dass die Bedrohungslage nach wie vor f
#252;r viele zu abstrakt ist. Neben der eigentlichen Bek
#228;mpfung der Cyberkriminalit
#228;t wird daher in Zukunft auch die Aufkl
#228;rung und Sensibilisierung f
#252;r dieses wichtige Thema zu den gro
#223;en Aufgaben des Staates gegen
#252;ber der Gesellschaft geh
#246;ren.
#8220;

Viele Akteure, aber wenig Expertise

Der Politikwissenschaftler gibt in seinem Buch einen
#220;berblick
#252;ber die Akteure, die in Deutschland beim Thema Cybersicherheit involviert sind: Das sind allen voran das Bundesministerium des Innern mit den Bundes
#228;mtern f
#252;r Sicherheit in der Informationstechnik sowie f
#252;r Verfassungsschutz und dem Bundeskriminalamt. Unterst
#252;tzung geben das Wirtschafts-, Verteidigungs- und Bildungsministerium, das Ausw
#228;rtige Amt sowie die L
#228;nder. Hinzu kommt das 2011 eingerichtete Nationale Cyberabwehrzentrum.
#8222;Die Koordinierung zwischen den einzelnen Ministerien und Einrichtungen, die f
#252;r die
#246;ffentliche IT-Sicherheit in Deutschland verantwortlich sind, ist in vielen Bereichen defizit
#228;r, da innerhalb der Ministerien oftmals nicht eindeutig geregelt ist, welche Abteilung f
#252;r das Thema zust
#228;ndig ist. Einige Ministerien bringen sich zudem nicht ausreichend in den Politikformulierungsprozess auf Bundesebene ein. Beim Bundesministerium der Verteidigung muss ganz grunds
#228;tzlich gefragt werden, ob es bereits im Cyberzeitalter angekommen ist. Weder organisatorisch noch strategisch wird es seiner Rolle als eines der nationalen Schl
#252;sselministerien in cybersicherheitspolitischen Belangen gerecht
#8220;, h
#228;lt Kullik in seiner Studie fest und er
#246;rtert:
#8222;Alle deutschen Sicherheitsbeh
#246;rden leiden unter einem allgemeinen Personalmangel an IT-Fachkr
#228;ften. Die Entwicklungsperspektiven f
#252;r angeworbene Spitzenkr
#228;fte aus der IT-Branche sind innerhalb deutscher Sicherheitsbeh
#246;rden nicht sonderlich hoch. Deutschland kann daher gegenw
#228;rtig bestenfalls als eine sich entwickelnde Cyber-Mittelmacht bezeichnet werden, dessen vorhandene Cyberf
#228;higkeiten momentan weit hinter den M
#246;glichkeiten der USA, Chinas, Russlands, Gro
#223;britanniens und vermutlich auch Frankreichs und Israels zur
#252;ckstehen.
#8220;

IT-Ausr
#252;stung statt milit
#228;rischem Gro
#223;ger
#228;t

Kullik formuliert als Konsequenz seiner Ergebnisse ein ganzes B
#252;ndel konkreter Handlungsempfehlungen. Dazu z
#228;hlt die Schaffung klarer Zust
#228;ndigkeiten und Verantwortungsstrukturen in den Cyber-Kernministerien und den flankierenden Ministerien. Zudem r
#228;t er zur Aufstockung des Personals in den Kernministerien und dem Nationalen Cyberabwehrzentrum sowie zur Schaffung eines Bundes-Cyberbeauftragten zur besseren Koordinierung netzpolitischer Themen auf Bundesebene. Grundlegend fordert der Politikwissenschaftler die Anerkennung des Cyberspace als strategisch wichtigen Raum f
#252;r nachrichtendienstliche und milit
#228;rische Computernetzwerkoperationen. Au
#223;erdem empfiehlt er unter anderem eine r
#252;stungspolitische Neuausrichtung
#8211; weniger milit
#228;risches Gro
#223;ger
#228;t f
#252;r die Bundeswehr, daf
#252;r eine bessere IT-Ausr
#252;stung der Sicherheitsbeh
#246;rden.

#8222;Jakob Kullik hatte das dr
#228;ngende Problem erkannt, lange bevor Edward Snowden die USA verlie
#223; und sich mit seinen brisanten Informationen an B
#252;rger und Regierungen wandte
#8220;, so Prof. Dr. Beate Neuss, Inhaberin der Professur Internationale Politik der TU Chemnitz, die die Forschung betreut hat.
#8222;Das historisch Neue sind die Dimensionen, in denen politische und industrielle Spionage, Kriminalit
#228;t und Sabotage betrieben werden k
#246;nnen. Neue Formen der Kriegsf
#252;hrung tun sich auf. Erst langsam ist diese Erkenntnis in wirtschaftliche Unternehmen und staatliche Stellen gedrungen. Umso entscheidender ist es, die Abwehrm
#246;glichkeiten zu er
#246;rtern und politisch-rechtlich zu analysieren
#8220;, sch
#228;tzt Neuss ein.

Bibliographische Angaben: Kullik, Jakob: Vernetzte (Un-)Sicherheit? Eine politisch-rechtliche Analyse der deutschen Cybersicherheitspolitik, Hamburg 2014. Verlag Dr. Kovac, Band 7 der Reihe
#8222;Chemnitzer Schriften zur europ
#228;ischen und internationalen Politik
#8220;, ISBN 978-3830076490, 284 Seiten

Kontakt: Jakob Kullik, E-Mail jakob.kullik@s2007.tu-chemnitz.de

<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=565405" width="1" height="1">

Pressekontakt

Technische Universität Chemnitz

09111 Chemnitz

Firmenkontakt

Technische Universität Chemnitz

09111 Chemnitz

Wer Fächergrenzen überspringen möchte, ein gut betreutes und praxisnahes Studium auf einem modernen Campus sowie besondere Forschungsbedingungen sucht, findet dies an der Technischen Universität Chemnitz. Hier sind Ingenieur- und Naturwissenschaften sowie Mathematik eng verknüpft mit den Wirtschafts-, Geistes- und Sozialwissenschaften. In diesem Klima entstehen gemeinsam mit der Industrie Spitzencluster in der Forschung, attraktive Bildungsangebote und internationale Netzwerke.