

Kleine Anfrage

der Abgeordneten Dr. Marcus Faber, Alexander Graf Lambsdorff, Jens Beeck, Dr. Jens Brandenburg (Rhein-Neckar), Sandra Bubendorfer-Licht, Dr. Marco Buschmann, Christian Dürr, Hartmut Ebbing, Daniel Föst, Otto Fricke, Thomas Hacker, Reginald Hanke, Peter Heidt, Katrin Helling-Plahr, Markus Herbrand, Torsten Herbst, Katja Hessel, Dr. Christoph Hoffmann, Reinhard Houben, Ulla Ihnen, Olaf in der Beek, Dr. Marcel Klinge, Daniela Kluckert, Pascal Kober, Konstantin Kuhle, Ulrich Lechte, Alexander Müller, Frank Müller-Rosentritt, Dr. Wieland Schinnenburg, Dr. Hermann Otto Solms, Dr. Marie-Agnes Strack-Zimmermann, Michael Theurer, Gerald Ullrich, Nicole Westig und der Fraktion der FDP

Cyber-Sicherheit von maritimen Navigationssystemen der Marine

Mit dem Fortschreiten der Digitalisierung der Kampfschiffe der Deutschen Marine wachsen neben den Chancen auch kontinuierlich die Gefahren durch eben diese Digitalisierung. Die Dimension Cyber- und Informationsraum ist nicht mehr nur eine Unterstützungsebene, sondern wird in heutigen Konflikten ein elementarer Teil der Wirkebene sein. Mit der Digitalisierung, Automatisierung und Vernetzung der Systeme auf den Kampfschiffen müssen diese Systeme auch robuster werden, um unter geänderten geopolitischen Bedingungen gegen neue hybride Bedrohungen und Cyber-Angriffe von Staaten und Organisationen gewappnet zu sein.

Aktuell warnt das Bundesamt für Verfassungsschutz (BfV) vor Gefährdungen wie Spionage und -sabotage hinsichtlich umfassender Navigationssysteme, sogenannter ECDIS (electronic chart display and information system) auf Schiffen (URL: <https://www.maritimes-cluster.de/news/aktuelles/sicherheitshinweises-des-bundesamtes-fuer-verfassungsschutz/>). In solchen Navigationssystemen kann die GPS-Navigation, das Radar, das Automatische Identifikationssystem, elektronische Seekarten, etc. integriert werden. Damit sind diese Systeme unabdingbar für eine uneingeschränkte, sichere sowie zeitgemäßer Navigation und damit auch der Einsatzbereitschaft der Kampfschiffe der Deutschen Marine. Insbesondere global agierende Hersteller von modernen, maritimen Navigationssystemen, so befürchtet der BfV, können in den jeweiligen „Herkunftsländern weitreichender Einflussnahme der dortigen Nachrichtendienste ausgesetzt sind“. Damit besteht auch die Gefahr, dass bei solchen kritischen Anwendungen für die Marine bereits bei der Programmierung aber auch bei späteren Updates der Software ein Risiko zur Kompromittierung besteht.

In Krisensituationen bestünde damit die Möglichkeit, dass die Position sowie Fahrt und Kurs von Kriegsschiffen feindlichen Kräften zur Verfügung steht. Dies bedeutet eine unmittelbare Gefahr für die Besatzung und wäre eine Einschränkung der Einsatzfähigkeit. Ein derartiges Einfallstor in das Netzwerk ei-

nes Kampfschiffes kann auch auf andere Systeme ausstrahlen. So besteht die Gefahr, dass ein möglicher feindlicher Zugriff auf die Navigationssysteme aufgrund der Vernetzung an Bord dazu führt, dass Zugang zu Sensoren, Effektoren und Steuerungssystemen erhalten werden kann (URL: <https://esut.de/2019/08/fachbeitraege/streitkraefte-fachbeitraege/14134/herausforderungen-der-cyber-sicherheit-in-der-deutschen-marine/>). Die Cyber-Sicherheit von Navigationssystemen der Marine ist damit von besonderer und kritischer Bedeutung für die Einsatzbereitschaft.

Wir fragen die Bundesregierung:

1. Sind bei Navigationssystemen der Deutschen Marine Firmen (inkl. Tochterfirmen) beteiligt, die Standorte in Ländern haben, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nr. 17 SÜG stehen?
Wenn ja, welche Firmen in welchen Ländern?
2. Sieht die Bundesregierung ein Risiko, dass auch die Marine von der obigen Warnung des BfV betroffen ist?
3. Welche Maßnahmen hat die Marine getroffen, um den Sicherheitshinweisen des BfV zu folgen?
4. Findet die Programmierung dieser Navigationssysteme von Firmen (inkl. Tochterfirmen) in Ländern statt, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nr. 17 SÜG stehen?
Wenn ja, welche Firmen in welchen Ländern?
5. Werden diese Navigationssysteme gezielt und regelmäßig nach Schadsoftware und ungewollten Funktionen überprüft?
6. Wurden die genannten Systeme von den zuständigen Stellen der Bundeswehr (z. B. Zentrum für Cybersicherheit, Zentrum für Softwarekompetenz, Zentrum für Cyber Operations) einmal auf mögliche Angreifbarkeit („Penetration“) getestet, bezüglich selbständiger Kontaktaufnahmen der Systeme nach außen geprüft, oder einer Code-Analyse unterzogen?
7. Wurde geprüft, ob diese Systeme die IT-Sicherheits-Anforderungen der Bundeswehr einhalten?
 - a) Wenn ja, wann, von wem, und mit welchem Ergebnis?
 - b) Wenn nein, warum nicht und existieren Hinderungsgründe?
8. Wurden Prüfungen der genannten Systeme von Dienststellen der Bundeswehr verhindert, zum Beispiel aufgrund rechtlicher Bedenken?
Wenn ja, mit welcher Begründung?
9. Wann wurden letztmalig die Implementierungs- und Wartungsverfahren dieser Systeme kritisch evaluiert?
10. Gab es in der Vergangenheit anlassbezogene Prüfungen der Navigationssysteme?
Wenn ja, wann und auf welchen Schiffen?
11. Werden die bereits bei der Marine verbauten Navigationssysteme durch Firmen (inkl. Tochterfirmen) in Ländern ferngewartet, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nr. 17 SÜG stehen?
12. Können diese Navigationssysteme grundsätzlich durch Firmen (inkl. Tochterfirmen) aus Ländern ferngewartet werden, die auf der Staatenliste im Sinne von § 13 Absatz 1 Nr. 17 SÜG stehen?

13. Hat die Bundeswehr uneingeschränkten Zugriff auf den Quellcode dieser Navigationssysteme?
14. Existieren sogenannte Blackboxen in diesen Navigationssystemen?
15. Wie werden die zuständigen IT-Offiziere der Marine ausgebildet und nach welchem Auswahlverfahren für das einzelne Kampfschiff ernannt?
16. Inwiefern werden Geheimhaltungsbereiche auf den Kampfschiffen der Deutschen Marine gesichert und kontrolliert?
17. Sind bei der Marine aktuell Navigationssysteme von Firmen (inkl. Tochterfirmen) verbaut, die vom Militärischen Abschirmdienst (MAD) oder dem Bundesamt für Verfassungsschutz als Prüf- oder Verdachtsfall geführt werden?
18. Laufen derzeit Ausschreibungen für neue ECDIS-Navigationssysteme für die Marine und wie ist der Stand der Ausschreibung bzw. Vergabe?
Wenn ja, für welche Kampfschiffe der Marine läuft die Ausschreibung?
19. Wurde die Warnung der Behörden vor möglichen Zugriffsmöglichkeiten auf die ECDIS-Systeme oder mögliche Sabotage dieser Systeme bei der Ausschreibung berücksichtigt und welche Maßnahmen wurden getroffen, um solche Zugriffe von Beginn an auszuschließen?
20. Hat der MAD oder das BfV wegen der laufenden Ausschreibung eine oder mehrere Prüfungen von möglichen oder tatsächlichen Anbietern eingeleitet?
21. Handelt es sich bei ECDIS-Navigationssystemen um sogenannte nationale verteidigungsindustrielle Schlüsseltechnologie?

Berlin, den 30. September 2020

Christian Lindner und Fraktion

Vorabfassung - wird durch die lektorierte Version ersetzt.