Analyses OSW

CENTRE FOR EASTERN STUDIES 9.01.2019 www.osw.waw.pl

# Hacking attack on German politicians

Kamil Frymark

On 6 January, Germany's Federal Criminal Police (*Bundeskriminalamt*, BKA) detained a person suspected of posting information online concerning about a thousand German politicians, including Chancellor Angela Merkel, as well as artists and journalists. The 20-year-old suspect pleaded guilty and is cooperating with the police. The stolen data was published on the social networking site Twitter, and was available from December 2018. According to a government spokesman, the data, from the period 2009-18, did not constitute a threat to national security, and included private addresses and phone numbers. Only around 50 instances were classified as 'serious', and concerned the disclosure of private correspondence, among other matters.

In response to the attack, the German government is planning changes at the Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*, BSI). Among other things, one unit of the BSI, the National Cyberdefence Centre, which deals with the coordination of information security at both the federal and provincial levels, is to operate on a continual basis, and not only in the event of an attack. Last October the Ministry of Internal Affairs announced an amendment to the 2015 Act on security in the IT sector, as well as an increase in the numbers of BSI employees by around 800 to 1300 people. Proposals for changes have also been presented by the justice minister Katarina Barley (SPD), which include the removal by social network sites of any accounts which are in violation of German law.

**Commentary**

- The rapid detention of the suspect and the first leaks from the investigation confirm the conviction predominant in media coverage that the group of perpetrators was small and had no connections with the activities of foreign intelligence services. The perpetrator's motives are unknown, but the initial thesis about a relationship with right-wing extremists (the material made publicly available has no links with the AfD) has not been confirmed by reports from the investigators. At the same time, the government has downplayed the idea that the BSI paid insufficient attention to the threat (this leak of individual data had been known about since the beginning of December), and is trying to marginalise the importance of the data that has been leaked. Nevertheless, its inattention to the BSI's warnings may attest to the ineffectiveness of the reforms to the IT defence system carried out after previous hacking attacks on Germany.

- One problem for Germany's IT defence system is its dispersion between different institutions at both the federal and provincial levels, as well as the lack of effective coordination between departments of the government's special services. Ensuring security would not only require expanded investment and changes to the law, but also changes to government structures. This will not be possible in the near future because the provinces (*Länder)* do not want to give up their existing powers. Furthermore, boosting IT capabilities will be difficult because of the problem of acquiring specialists for administration, for reasons including the competitive offers these people receive from private companies.
- The interior minister Horst Seehofer (CSU) shoulders the responsibility for the slow pace of actions taken by the departments subordinate to him, primarily the BSI. Both the opposition and the co-ruling SPD have accused him of failing to respond quickly enough, and of focusing on the ministry's work on migration issues. This will mean a further weakening of Seehofer's political position.