Germany’s IT Security Act 2.0: Another step towards a police state

Wolfgang Weber
22 April 2019

Just a few days after the publication of a draft for an “Intelligence Enabling Act,” the German interior minister Horst Seehofer has submitted proposals to the cabinet for a comprehensive extension and tightening up of the 2015 IT Security Act.

The “IT Security Act 2.0” would allow the Federal Office for Information Security (BSI) to carry out intelligence tasks, expand the powers of the police and extend criminal law by introducing new criminal offences. The platform www.netzpolitik.org published the draft on March 27.

Until now the main work of the BSI was to ward off attacks on the IT system, such as to inform the public about viruses and trojans, draw attention to security gaps in well-known programs such as Windows, Office and Adobe Flash and close such security gaps. Now, on the pretext of protecting the public interest, the BSI is to be upgraded into an offensive agency capable of cracking, hacking and manipulating IT systems, private databases and networks.

In the future the BSI will be able to use systematic scanning of identifiable portals (device access) to search for insecure, i.e., vulnerable devices. In the so-called Internet of Things such devices include internet-connected refrigerators, washing machines, cameras, automobiles, even children’s computers or baby monitors, through which an attacker could penetrate the WLAN of a business or individual.

The BSI will be allowed to log onto such devices to detect passwords and then spy on, and also change data. Actions that up to now are punishable are thus legalised in the case of the BSI. In addition, telecommunication providers are required to submit to the BSI the personal data corresponding to an IP address.

The Federal Office may inform affected owners of insecure IT systems or systems that have been broken into, but need not do so. In addition, it can alter devices, networks and IT systems that it has classified as “insecure.” To this end the BSI can oblige telecommunications providers to install software patches developed by the BSI on a system registered under a specific IP address to delete or change “malware.”

The ability to secretly infiltrate and manipulate IT systems allows the security forces to act against, and even manipulate evidence against individuals and organisations deemed to be “suspicious” or “anti-constitutional.” This constitutes a radical breach of basic democratic rights such as the inviolability of the home, telecommunications security, the right of self-determination and the privacy of those affected and, depending on the target, a possible violation of the freedom of the press or the confidentiality rights of doctors and lawyers.

The Interior Ministry has justified IT Security Act 2.0 by claiming it allows security agencies to protect “insecure systems” from attackers and take control of groups of remote-controlled devices—so-called botnets—to prevent them undertaking attacks or sending spam. The ministry is deliberately concealing the fact that protection against botnets is also possible in other, defensive ways to secure, for example, critical infrastructure such as the energy or water supplies, or railway networks.

Paragraph 163g, located at the very end of the draft, makes clear the dictatorial aims hidden behind the mask of “IT security.” It allows prosecutors and the police the right “to access the user accounts or functions” of a suspect, against his or her will, and “contact third parties using this virtual identity.” The draft continues: “The suspect is required to provide the access data required to employ the virtual identity.”

A general, and not a concrete suspicion that someone has committed a crime, plans to commit one, or is participating in a crime with the help of an internet service, is sufficient to force that person to hand over their account details. Should he or she refuse, they can be detained for up to six months under Section 70 of the Criminal Code.

Among the crimes that are supposed to provide the pretext for state intervention are a long list of offences, ranging from "abduction to falsifying an asylum claim" (i.e., helping a refugee) and murder, but also minor everyday offences such as abuse via email or Ebay fraud. The list provides ample opportunity for arbitrary searches and raids, along with "covert investigations" on the internet.

The draft also states that, "Accounts ... can be taken over and used even if the government agency obtains the access data in other ways, for example by means of covert investigations or as part of an online search," e.g., through the deliberate use of trojans.

Finally, the IT Security Act 2.0 stipulates a number of new offences, while other criminal law provisions are tightened up considerably. For a whole range of existing crimes, such as spying, intercepting or manipulating data, the maximum penalty is increased from two to five years imprisonment. This does not apply, of course, when the perpetrators are the BSI, the intelligence services or the police.

These same offences are now upgraded to the level of serious offences, permitting the authorities to not only listen into telephones during an investigation, but also deploy so-called state trojans, i.e., spyware and malicious software developed by the BSI or other state agencies.

A new offence has been created of providing "Internet-based services" that make it possible or easier to commit crimes via internet services. This is directed against trading platforms in the so-called Darknet, but also against services offering anonymity or private communication spaces such as the TOR browser. This is another assault on basic democratic rights, such as the right to the self-determination of information and freedom of expression, of which the right to anonymity is crucial.

In future, it will also be a criminal offence to publish or plan to publish private data, with a penalty of up to 10 years. A particularly serious case of such a crime exists if the act "threatens serious disadvantage for the Federal Republic of Germany." This could undoubtedly include such acts as publicising leaked data revealing, for example, the involvement of the German army in war crimes in Afghanistan or Mali.

The draft also makes "digital trespassing" or, as it is called in the bill, the "unauthorised use of IT systems," a criminal offence. This would include infiltrating a government database for the purpose of disclosing state crimes, as Chelsea Manning did in 2010 when she transmitted to the world, via WikiLeaks, American military documents exposing US Army war crimes in Iraq and Afghanistan.

The last two clauses in particular clearly show that the IT Security Act 2.0 must be seen in connection with the arrest of Julian Assange and his imminent extradition to the US. Anyone who, like Chelsea Manning and Julian Assange, stands up for democratic rights and exposes imperialist crimes is to be intimidated, punished and silenced.

A host of lawyers in the various ministries are now working feverishly, and often in grotesque detail, to concretise the future laws governing the activities of the police and intelligence agencies. They seek to neatly sew up the "legal" abolition of democratic rights in order to preserve the appearance of a "rule of law" as long as possible. The German judiciary has considerable experience in this sort of planning for dictatorship, and not just from the monarchy before 1918 and the Weimar Republic. Without the active collaboration of leading judicial figures, the dictatorship of Hitler, the persecution of the Jews and their extermination would not have been possible.

The speed with which similar work is now being undertaken is breath-taking. It corresponds to the global intensification of the class struggle against social inequality, militarism and dictatorial regimes. These class struggles are the main reason why the ruling classes in Germany, Europe, and also the US, are increasingly turning towards dictatorship and fascism.

To contact the WSWS and the Socialist Equality Party visit:

wsws.org/contact

© World Socialist Web Site