New hacking powers for German intelligence agencies - about:intel

Santino Musillami ⋮ 14-18 minutes ⋮ 10/27/2020

Without convincing evidence, the German government wants to expand surveillance powers for the intelligence services. However, the marginal changes proposed to the oversight framework cannot make up for this. We show that the draft law fails to meet international good oversight standards and would, with the introduction of the so-called "state trojan", undermine IT security for all. Germany should not miss this opportunity to bring its intelligence legislation up to democratic standards.

This week, Angela Merkel's ruling coalition of Conservatives and Social Democrats decided to push through a draft law that makes a series of changes to existing German intelligence legislation. The bill includes highly controversial provisions on hacking powers and some half-hearted changes to the G10 Commission, the competent oversight body that works in an honorary capacity.

After lengthy negotiations this decision was part of a larger political horse trade that included several other none-intelligence related aspects, such as conducting a study on racism in German police forces. The bill (available in German only) still needs to be passed by parliament.

The key sections of the bill would amend the G10 Act, Germany's intelligence law that applies to all three federal intelligence agencies as well as to the 16 local intelligence services in Germany's federal states. It comes at a time when a larger reform of the BND law, which regulates foreign surveillance and intelligence sharing, is also in the making.

The federal interior ministry, led by the conservative CSU, had made a first, much more ambitious and controversial legislative proposal back in April 2019. After an initial "No" from the ministry of justice, which is under Social Democratic leadership, the discussion about the legislative initiative got stuck in closed door negotiations among government policy makers.

In June 2020, the new draft law became public. It is much thinner, but still includes an equipment interference capability, dubbed "Quellen-TKÜ" in lovely German legalese. At first, this new bill, again, hit strong opposition from Merkel's coalition partner, the Social Democrats, spearheaded by their party leader Saskia Esken. This disagreement has now reportedly been overcome and the adoption

of the bill by the Bundestag appears to be a done deal among the coalition partners.

The bill contains some approaches to professionalise the G10 Commission, but these remain fragmented and fall short of what would be needed and is already practiced in other democracies. At the same time, a lawsuit against said G10 Act is pending before Germany's constitutional court. It seems likely that an overhaul of the G10 Act will be needed after the court will pronounce its judgement on this constitutional complaint.

Based on a statement that we submitted in an earlier consultation process, this article will discuss parts of the proposed legislation. We summarise the central points of critique and, based on our research, propose a few concrete steps to improve this draft law.

Resources of the G10 Commission

The G10 Commission is the oversight body in charge of authorising applications for surveillance brought by the intelligence services. The bill would increase the G10 Commission by one additional member and one additional deputy member. It is also envisaged that at least three members and three deputy members must be qualified to hold the office of a judge. Both steps are to be welcomed in principle. However, the G10 Commission has been working at its capacity limits for some time. Now that the hacking capability will be added, a new surveillance power that the G10 Commission has no experience in overseeing, an increase in personnel is more than overdue. The recent ruling of the Federal Constitutional Court on the BND Act has emphasised that independent, judicial oversight is key to guarantee proportionality. In order to protect the fundamental rights of those affected, the capacities of the G10 Commission should therefore be strengthened beyond the steps envisaged in the bill.

The G10 Commission works on an honorable basis. This is no longer appropriate. There is a severe mismatch between the low level of professionalisation of the G10 Commission and the fast-paced evolution of the intelligence services themselves. The planned increase in the number of commission members is not sufficient to deal with the capacity bottlenecks. Given the growing importance of communications interception in our digital society, ensuring an effective approval process for the interception of communications is a full-time job. In its ruling on the BND Act, the Federal Constitutional Court agreed and once again found oversight exercised on an honorable basis to be insufficient. Rather, the court stated that "control needs to be technically competent and professionalised and ensured by full-time staff".

What is more, independent reporting would strengthen public confidence in the G10 Commission. In the Netherlands, for example, public reporting obligations

have long been standard practice: the TIB, the body responsible for approving surveillance measures, recently stated in its report, which is available in English, that it had examined “a total of 2,159 applications in the period from 1 May 2018 to 1 April 2019”. The report shows, among other things, how often applications were found to be unlawful and for what reason they were rejected. In order to increase transparency, the German draft should therefore include an independent reporting obligation for the G10 Commission.

Direct access for the G10 Commission

Germany also has to catch up in the area of data-driven intelligence oversight. In the UK, the Netherlands, France, Switzerland, Denmark, Norway and Sweden, the respective oversight bodies have direct access to the databases of intelligence services and can autonomously retrieve and evaluate data. This has not been the case in Germany so far.

The fact that the draft law now includes direct access by the G10 Commission to automated files of the federal intelligence services is therefore a step in the right direction. Such direct access is the basic prerequisite for modern intelligence oversight. Especially the conditions for the use of hacking tools need to be overseeable. Without direct data access, this is not possible. However, the specifications in the present draft law are still wanting.

Specification of data types for effective and focused oversight

The bill does not specify which types of data the G10 Commission may access. However, this is important as not all data is equally useful for oversight. The evaluation of log files and metadata, as is the case in Denmark for example, can enable effective oversight without jeopardising confidentiality. Other data is often less informative for oversight committees. More concrete stipulations in this respect would thus both ensure more effective and focused oversight and guarantee that the intelligence services do not have to keep irrelevant records and redundant controls are avoided. A study by the Stiftung Neue Verantwortung (SNV) on data-driven intelligence oversight that we produced with help from the European Intelligence Oversight Network, breaks down which types of data and which associated supervisory tools are particularly relevant for effective administrative control and how this is practiced in international comparison.

Further develop technical expertise for the G10 Commission

The oversight activities of the G10 Commission are becoming increasingly technically demanding. The fact that the G10 Commission members would, according to the draft law, in the future be able to jointly appoint a “technical

advisor" who can participate in meetings and controls is a step towards establishing the needed technical competence of the G10 Commission. International comparison shows that additional external advice for judicial oversight plays an increasingly important role in many countries. The US, Great Britain, and New Zealand have also already made it possible for inspectors to obtain external expertise on technical issues at any time.

Due to the complexity of the intelligence agencies' information systems, more technical competence and resources are urgently needed in oversight to make good use of direct data access. This would also prevent an over-reliance on the expertise of the services themselves when reviewing them.

Technical expertise is also necessary in order to independently verify the technical specifications required in Para 11 (1a) of the bill. These so-called "technical assurances" say that only current communications may be monitored and recorded and that interferences in IT-systems are to be kept at the necessary minimum. It also includes a protection against unauthorised use, modification, or deletion of data "according to the state of the art" (also in Para 11 (1a)). But such requirements need independent evaluations of the technical possibilities. It is questionable whether one technical advisor alone can meet these needs for expertise. Therefore, it would make sense to provide the G10 Commission with access to further technical expertise, as is already available in other countries.

Duty to report errors for telecommunications providers

So far, Para 11 (2) of the G10 Act foresees that postal and telecommunications providers are obliged to cooperate and are informed about the end of surveillance measures. However, since the participating companies play a central role in the implementation of interception measures, they should be much more closely involved in the work of the oversight bodies. This is because oversight bodies such as the G10 Commission know far too little about the concrete implementation of approved warrants. The bill should therefore be supplemented by an error reporting obligation for service providers.

Under the British IP Act, for example, telecommunications service providers have long been obliged to report irregularities, such as incorrect data collection, to the UK oversight body IPCO as well as the relevant security authority.

The participating providers also have a need for legal certainty and the rule of law. In the USA, telecommunications companies have the possibility of appealing against surveillance orders before the FISC. The German bill should be supplemented by such a right to challenge intelligence warrants.

Some service providers have tried to sue the government because of mistakes and inconsistencies in the implementation of surveillance orders, but failed in their attempts before the Federal Administrative Court.

It would be an enormous gain for ensuring the lawful implementation of surveillance measures if ISPs would have an effective right to challenge warrants and other data collection orders. This already exists in the USA and the UK and would strengthen confidence in the proper and legally compliant implementation of interception measures.

Lack of safeguards for the use of equipment interference

The hacking power foreseen in the draft law ("communications surveillance on end user devices") is an operational, highly invasive measure that would allow all German intelligence services to access and manipulate communications data on all electronic devices, such as smartphones and laptops.

The safeguards provided for in the draft law are most likely not sufficient to comply with necessity and proportionality standards. In a comprehensive analysis, an independent expert working group has published a list of structural and operational minimum standards for using hacking tools. Hardly any of them are included in the current bill.

The draft law substantially contradicts the promise made in the government coalition agreement to strengthen IT security. The reason for this is that providers of postal and telecommunications services will be obliged to support the application of surveillance software if the intelligence services require it. Such measures, including redirection to websites prepared by the intelligence services that install spy software, could possibly lead to a reluctance among citizens to install security updates and undermine trust in the integrity of telecommunications providers. However, these are elementary components of IT security, and thus of public safety, in Germany.

In addition, the German government has so far neither made the Federal Office for Information Security more independent (although this was announced in the coalition agreement) nor has it introduced a government vulnerability management system. Equipment interference measures are based, among other things, on vulnerabilities that, according to German IT security law, are to be closed by the respective manufacturers. According to the present draft law, however, the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz*; the domestic intelligence agency*)*, along with the other German intelligence services, would be allowed to exploit these vulnerabilities in the future. Introducing an appropriate vulnerability management system and strengthening the independence of Germany's IT security agency would be basic prerequisites for counteracting this conflict of interests.

As a final point, the lack of empirical evidence at the core of introducing these additional surveillance powers should be noted. For several years, the German law enforcement agencies have had the authority to carry out equipment interference measures. As long as we do not know whether the use of hacking tools by law enforcement was effective, an intrusive surveillance power of this kind should not be expanded to all intelligence services.

Conclusion

It is not surprising that this bill was received with widespread criticism from business associations, civil society organisations and researchers. In order to justify the expansion of surveillance powers for the intelligence services, convincing empirical evidence for the operational need of said powers would be required. Yet, that evidence is missing.

The marginal changes to the oversight framework cannot make up for this. Bringing the G10 Commission up to speed and living up to international good oversight examples will require more, as we have shown.

Although this bill will likely be passed by parliament without significant changes, future litigation might probe its compliance with basic legal standards and human rights. In our view, the safeguards included in the draft law are flimsy and insufficient. The introduction of the so-called “state trojan” undermines the goal to create better IT security for all. Thus, the case for why German spies would need such new powers remains unconvincing.

Germany still has important work to do to bring its intelligence legislation up to democratic standards. Not taking those crucial steps now is a missed opportunity.

This research was funded by the Deutsche Forschungsgemeinschaft (DFG, German Research Foundation – Project Number 396819157).

Previous Chapter Next Chapter