Germany's secret role in repressive state spying

12 December 2014

Germany is seen by many as the place where the Snowdon revelations have had the greatest impact. But sometimes it seems the benchmark is somewhat skewed. While concerned citizens here feel disturbed by the revelations, in other parts of the world the consequences of government surveillance include arrest, torture and death. As with arms exports, Europe and in particularly Germany are helping to provide repressive regimes with the technology they need and are managing to do so without provoking much opposition at home.

The "surveillance business model" is how this is described by Dietmar Kammerer in the October Edition of Le Monde Diplomatique. Everything governments need to monitor the communications of an entire population, he writes, can now be easily obtained on the free market. It's a market that's growing; annual turnover from spy software is now estimated to amount to five billion US dollars.

Together with Reporters without Borders, Bahraini human rights activists and British civil rights lawyers from Privacy International, we at ECCHR have been working for years on legal action against the firms involved, in particular against German-British companies Gamma International and Trovicor.

The proceedings concern among other things the supply of the spy software FinFisher to Bahrain. The software enables Bahraini authorities to monitor computers remotely. Human rights activists, journalists and oppositionists in Bahrain continue to be subjected to systematic surveillance, detention, persecution and torture. Gamma has refused to comment on the export of the Trojan. Last summer, however, hackers detected FinFisher on the computers of Bahraini oppositionists, including some who are living abroad. In 2013 ECCHR turned to the OECD complaint process – admittedly not one of the strongest legal weapons. Our aim was to get the companies to admit to and halt the export of the software. The German National Contact Point, the authority responsible for these complaints, is embedded in the Federal Ministry for Economic Affairs. The Ministry prizes the expansion of exports as its ultimate objective; human rights complaints tend not to find a sympathetic ear. The Contact Point tends to be biased in its approach and often discontinues cases without conducting any further investigations – as it did last year in the case of German firm Trovicor. But the OECD contact point in England is run differently, and our British colleagues are hopeful that a strong statement will be issued against the export of these kinds of technologies.

German prosecution authorities rarely act in such cases, due to the difficulty in proving the supply and use of software for purposes that violate human rights. With this in mind, we were glad when hackers uploaded internal Gamma communications to the internet. The data showed not only that assistance was being provided to customers in Bahrain, but also revealed that computers in Germany were among those being targeted. It's fair to assume that in providing technical assistance, Gamma employees would easily be able to determine the whereabouts of the person being targeted by the spyware. The program displays the name of the individual targets alongside the flag of the target's country of residence.

We felt this new information would surely be of interest to the state prosecutor in Munich, the federal state with jurisdiction over Gamma, and submitted a criminal complaint in mid-October. Less than six weeks later the authorities informed us that they will not even attempt an investigation. The justification given is concise and blunt: never trust a hacker!

Information from hacked data was used to support our claims and we had the nerve to expect that this would prompt the prosecutors to examine the case further! The authorities countered our request with assurances that using the software in the way we claimed and as evidenced by the company's own internal documents is "strictly prohibited in the firm's terms of contract". That's good to know, we'll pass this on to our colleagues in Bahrain who have been imprisoned and tortured. Clearly it was all just a mistake – after all, such behaviour is contractually forbidden.

The state prosecutors additionally argued – remember, never trust a hacker! – that the law against secret surveillance is aimed only at hackers and "not at a state accessing data via telecommunications".

We will appeal the decision of the state prosecutors in Munich and continue to push for an investigation. It would help matters somewhat if German critics of state spying would also turn their attention to the plight of those who are currently suffering most under such surveillance.