Abstract: Deliberately weakened ciphers are of great interest in political discussion on law enforcement, as in the constantly recurring crypto wars, and have been put in the spotlight of academics by recent progress.

In this talk I will discuss recent results in the construction and deconstruction of backdoors in symmetric ciphers. First, I will talk about a result from Eurocrypt 2021 that showed a strong indication that the security of the widely-deployed stream cipher GEA-1 was deliberately and secretly weakened to 40 bits in order to fulfil European export restrictions that have been in place in the late 1990s. I will also explain one way how this backdoor might have been constructed, which requires some neat details in the understanding of Galois LFSRs.

Next, I will discuss the MALICIOUS design framework, published at CRYPTO 2020 by Peyrin and Wang, that allows to construct tweakable block ciphers with a backdoor, where the difficulty of recovering the backdoor relies on well-understood cryptographic assumptions. The constructed tweakable block cipher however is rather unusual and very different from, say, general-purpose ciphers like the AES.

By generalizing MALICIOUS I will explain how to construct backdoored tweakable block ciphers that follow modern design principles for general-purpose block ciphers, i.e., more natural-looking deliberately weakened tweakable block ciphers.

This talk is mainly based on joint work with Christof Beierle, Tim Beyne, Patrick Derbez, Patrick Felke, Gaëtan Leurent, Håvard Raddum, Yann Rotella, David Rupprecht, and Lukas Stennes.