CSCI 180 Homework 2

Please read the following scenario and answer the question to the best of your ability. This assignment will not be graded based on your correct/wrong answer, but just based on your submission and demonstrating effort.

Security researchers often use conference platforms such as DefCon and RSA to announce newly discovered security tools or vulnerabilities; often these are controversial, and invite careful ethical reflection on the harms of benefits of such disclosures, and the competing interests involved. Here are two examples to compare and consider from an ethical standpoint:

A) At DefCon 2016, security researcher Anthony Rose presented the results of his testing of the security of products in the emerging market for Bluetooth-enabled door locks.9 He found that of 16 brands of locks he purchased, 12 had profoundly deficient security, including open transmission of plain-text passwords, the ability to easily change admin passwords and physically lock out users, and vulnerability to replay attacks and spoofing. Some of the locks could be remotely opened by an attacker a half-mile away. Of the manufacturers Rose contacted, only one responded to his findings. Another shut down its website but continued to sell its product on Amazon.

B) At Defcon 2017, two members of Salesforce's "Red Team" of offensive security experts were scheduled to present (under their Twitter handles rather than their professional names) details of their newly developed security tool, Meatpistol. Meatpistol is an automated 'malware implant' tool designed to aid security red teams in creating malware they can use to use to attack their own systems, so that they might better learn their own systems' vulnerabilities and design more effective countermeasures. It functioned more or less as any malware tool does, able not only to generate code to infect systems but to steal data from them, except that it reduced the time needed to create new forms of such code from days to mere seconds. The two members of Salesforce's offensive security team planned to make Meatpistol's code public after the event, with the view that making Meatpistol an open source tool would allow the community of security researchers to improve upon it further. As with any malware implant tool, however, making it open source would have inevitably invited other hackers to use it for malicious purposes. Just prior to the event, an executive at Salesforce instructed the team not to release Meatpistol's code, and shortly thereafter, instructed them to cancel the previously-approved presentation altogether. The team presented on Meatpistol at DefCon anyway, after which they were summarily fired by Salesforce. Meatpistol's code was not released.

Question: Considering the ethical similarities and differences between these two scenarios:

1. Do you think the 2016 Rose presentation was ethical, all things considered? Why or why not?
2. What about the 2017 Meatpistol presentation (including its planned code release) – was it ethical? Was Salesforce right to try to stop it, and to block the code release?