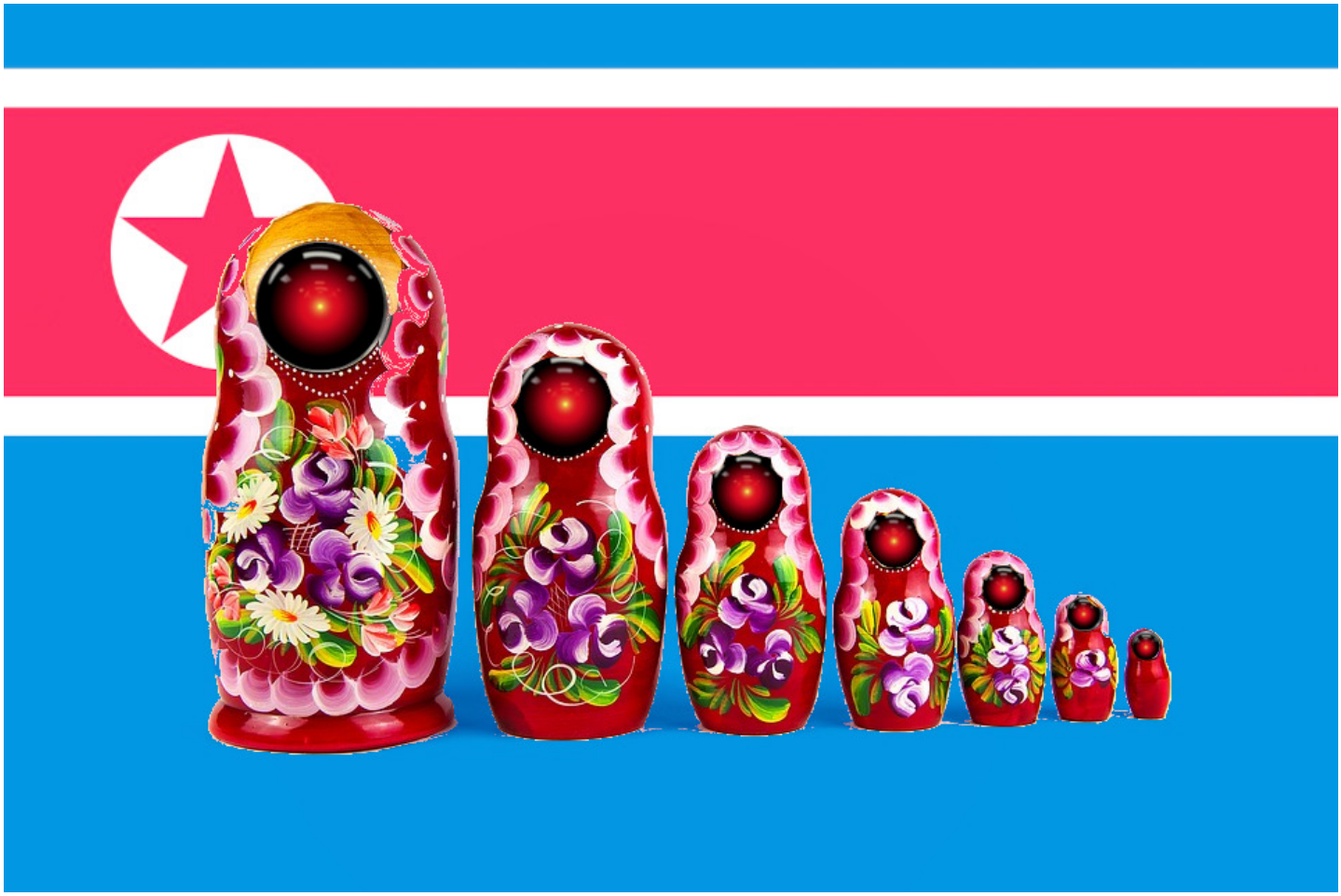
Twitter Thread by Cory Doctorow #BLM

Cory Doctorow #BLM
@doctorow

One of the most fascinating revelations from the Snowden documents was the story of "fourth party collection," which is when the NSA hacks the spy agency of a friendly nation to suck up all the spy data it has amassed on its own people.

https://t.co/8WZ6WJigjU

1/



It's a devilishly effective spying technique and it surfaces a major risk of mass domestic surveillance - if your internal police get hacked by another nation, then that country can get all of your data. The secret police say they're spying to protect you - some protection!

2/

Even more mind-blowing is the existence of "fifth-party collection" (spying on a spy agency that's spying on another spy agency) and "SIXTH-party collection" (spying on a spy agency that's spying on another spy agency that's spying on another spy agency) .

3/

It's also fascinating because it's so obvious in retrospect. Willie Sutton robbed banks "because that's where the money is." Spooks spy on other spooks because that's where the kompromat is: gathered, sorted, filed and analyzed.

4/

This week, Google's Threat Analysis team published a warning to security researchers to be vigilant about a sophisticated threat-actor that is targeting the infosec community.

https://t.co/dlueiQsDbK

5/

Google says the attacker is working from North Korea (which strongly implies that they are working on behalf of the DPRK itself).

6/

An analysis of the attack recounts how the hackers would ingratiate themselves to infosec professionals, ask them to collaborate on interesting problems, and then slip them a poisoned software library that would take over their systems.

https://t.co/ne0Oyiri90

7/

Like fourth-party collection, this is a highly leveraged attack. Security researchers tend to have a lot of proof-of-concept malware, notes on vulnerabilities, and other juicy tools and intel that could be weaponized to attack high-level systems.

8/

Image: Cryteria (modified)
https://t.co/ICebVcdH1f

eof/