MONDAY: A DIFFERENT ARK

[*Caution: some content in this video is NSFW*] Today's Monday Movie is a short film by Patrick Cederberg published three years ago. This short reflects the love life of a youth whose age is close to that of my two kids. A few things have changed in terms of technology used — I don't think either Facebook or Chatroulette is as popular now with high school and college students as it was, but the speed of internet-mediated relationships is the same. It's dizzying to keep up with kids who are drowning in information about everything including their loved ones.

Their use of social media to monitor each other's commitment is particularly frightening; it's too easy to misinterpret content and make a snap decision as this movie shows so well. Just as scary is the ease with which one may violate the privacy of another and simply move on.

Imagine if this youngster Noah had to make a snap decision about someone with whom they weren't emotionally engaged. Imagine them using their lifetime of video gaming and that same shallow, too-rapid decision-making process while piloting a drone.

Boom.

Goodness knows real adults with much more life experience demonstrate bizarre and repeated lapses in judgment using technology. Why should we task youths fresh out of high school and little education in ethics and philosophy with using technology like remote surveillance and weaponized drones?

Speaking of drones, here's an interview with GWU's Hugh Gusterson on drone warfare including his recommendations on five of books about drones.

A, B, C, D, USB…

- USBKiller no longer just a concept (Mashable) —$56 will buy you a USB device which can kill nearly any laptop with a burst of electricity. The only devices known to be immune: those without USB ports. The manufacturer calls this device a "testing device." Apparently the score is Pass/Fail and mostly Fail.
- Malware USBee jumps air-gapped computers (Ars Technica) — Same researchers at Israel's Ben Gurion University who've been working on the potential to hack air-gapped computers have now written software using a USB device to obtain information from them.
- Hydropower charger for USB devices available in 2017 (Digital Trends) — Huh. If I'm going to do a lot of off-grid camping, I guess I should consider chipping into the Kickstarter for this device which charges a built-in 6,400mAh battery. Takes 4.5 hours to charge, though — either need a steady stream of water, or that's a lot of canoe paddling.

- Arizona and Illinois state elections systems breached (Reuters) — An anonymous official indicated the FBI was looking for evidence other states may also have been breached. The two states experienced different levels of breaches — 200K voters' personal data had been downloaded from Illinois, while a single state employee's computer had been compromised with malware in Arizona, according to Reuters' report. A report by CSO Online explains the breaches as outlined in an leaked FBI memo in greater detail; the attacks may have employed a commonly-used website vulnerability testing application to identify weak spots in the states' systems. Arizona will hold its primary election tomorrow, August 30.
- Now-defunct Australian satellite communications provider NewSat lousy with cyber holes (Australian Broadcasting Corp) — ABC's report said Australia's trade commission and Defence

Science Technology Group have been attacked frequently, but the worst target was NewSat. The breaches required a complete replacement of NewSat's network at a time when it was struggling with profitability during the ramp-up to launch the Lockheed Martin Jabiru-1 Ka-band satellite. China was named as a likely suspect due to the level of skill and organization required for the numerous breaches as well as economic interest. ABC's Four Corners investigative reporting program also covered this topic — worth watching for the entertaining quotes by former CIA Director Michael Hayden and computer security consultant/hacker Kevin Mitnick in the same video.

- Opera software users should reset passwords due to possible breach (Threatpost) — Thought users' passwords were encrypted or hashed, the browser manufacturer still asks users to reset passwords used to sync their Opera accounts as the sync system "showed signs of an attack." Norwegian company

Opera Software has been sold recently to a Chinese group though the sale may not yet have closed.

That's a wrap for now, catch you tomorrow! Don't forget your bug spray!