Q&A – 27 May 2021 – Prof. Gisela Bichler

1. **New tec like deep fake films are also a risk. Who is the person behind a message/information?**

   Media channels may differ in their susceptibility to host, and become inundated, with deep fake films could constitute *risky information settings* if the content of the misinformation puts people at risk for crime.

2. **The way you have conceptualized the interaction between physical and cyber space raises some interesting questions about prevention and enforcement. For example, are there organizations that can minimize, say, bullying or hacking? When DARPA first experimented with the Internet back in the 1970s, they rejected it as being too insecure (I believe they then created a closed network). Moderating social interactions could minimize bullying (e.g., people who do it are kicked off the stream). In short, do you have any ideas about organizing these networks to minimize negative effects?**

   There are many ways to develop intervention strategies that involve cyber settings. For example, place managers, human or algorithmic, can intervene to prevent victimization, to halt crime in progress, and to reduce harm post-attack. To illustrate, recently during a live flight simulator demonstration on Twitch, a moderator intervened and ejected a viewer who began making hateful and threatening statements towards a transgendered host who was conducting the demonstration while interacting with hundreds of viewers. To facilitate effective place management, all users should be required to sign a virtual code of conduct when registering for an account. A virtual code of conduct empowers place managers to act.

3. **Could we think the notion of cybercrime through the harm is imposed to the victim?**

   Yes. It is feasible that riskiness be measured as potential harm. For example, when ranking personal data breaches, the nature of (e.g., targeting employment records and tax identification numbers) and number of attacks a class of systems face could be used to calibrate the riskiness of campuses. An example of a class or set of systems might be university intranets.

4. **Some cyber places, especially cybercrime-related ones, are volatile as opposed to physical places. How does this affect law enforcement interventions? And how would this affect the reliability of those hyperspace maps you referred to?**

   I am not entirely sure what is meant by the term “volatile” in this question. Is this a reference to the ‘temporary’ nature of accounts. For example, a person sets up an account on a cybermarket place to quickly sell some stolen goods. After a few days, the account is deactivated or abandoned. If so, the issue is not to implement situational crime prevention measures that target a specific user; instead, target the vulnerabilities of the system (account set-up and authentication) to make it much harder to use for pawning stolen goods. Think of open-air drug markets. Removing a single dealer does not disrupt the market if the ecosystem supporting trade continues to operate. Cyber

environments are similar. We need to address the system features that generate crime opportunities to generate the maximal crime prevention benefit. If instead the goal is to investigate and prosecute specific individuals, this is not crime prevention.

5. **Not really a question, but an observation that you may have an opinion on. We have quite a number of incidents of physical bullying (beatings, really) at schools that were captured by the bystanders. These video clips are then shared online, so in a sense the person is being bullied in real life, and then again in the cyber world.**

   This is a good example of why hyperspace is so important. Over the past decade the amount of human behavior that routinely crosses domains has increased to the point that I wonder how much purely "physical" or purely "cyber" behavior remains.

   Think about your daily life. Do any aspects of your professional or personal life exist purely in the physical domain? I was reminded of this issue when my campus suffered a system outage. The source of the problem was not disclosed, but with the onset of cloud technologies and campus Wi-Fi, the system is no longer purely an intranet system with internet capabilities, and when it crashes, we cannot even operate the phones, regulate classroom climate, teach (all classrooms are smart), or even print (the desktops are no longer connected directly the printers sitting beside them). The failure was so all encompassing, the campus had to be evacuated following emergency protocols. We were under the illusion that campus life was still operating primarily in the physical domain. It is not so. All infrastructure exists in hyperspace.

   Returning to the issue of bullying. If students are standing around in the hall, witnessing an attack and simultaneously reporting on Instagram while at the scene, the divide between physical and cyber worlds is immaterial. The initial victimization occurs in hyperspace, where the domains intersect. Fallout and subsequent actions in both domains may (a) extend or escalate harm, (b) foster new victimization by the same or other bullies, (c) spread bullying (as people defending or standing up for victims are attacked), or (d) reduce harms (others deny the bully benefits from the crime). Intervention strategies would have to include a set of elements, some of which must be able to cross over as well. Interventions targeting one domain only would be ineffective.

6. **I wonder if redesigning the Internet so as to automatically identify where messages come from (to avoid people phishing and hiding behind multiple IDs). In that way, accountability can be increased. Thoughts?**

   I do not know enough about the system to comment on whether unilateral action to redesign the Internet is feasible. With this said, many systems and platforms are moving to duo two party authentication, adding account information requirements that could easily be used to cross validate/merge data between systems or platforms, and requiring regular account reactivation. If the most used and critical systems adopt these changes quickly, for a time at least, there will be an increase in accountability.