Introduction

We are entering an age where everyone can buy devices with encryption turned on out of the box[1]. For law enforcement, this encryption will make it harder to identify, track, and monitor criminal activity. When considering the priority the threat of terrorism, the targeted application of physical practical tools is considered most suitable.

Compared to political discussion to introduce backdoors into encryption and devices, the use of physical practical measures will be more successful, will remain useful for the long term, and will avoid any political cost. To increase trust in governments, it is recommended that the creation of backdoors in encryption and devices should be ruled out, qualified with description and direction to use strong alternative measures as described herein.

	Physical surveillance	**Targeted hacking**	**Communication Monitoring**
Terrorists	Yes	Yes	Yes
Transnational Organised Crime	Sometimes	Yes	Yes
Other less violent crime, and less sophisticated criminals	No	Sometimes	Yes

Figure 1: Matrix showing where the most expensive and direct targeting approaches are directed

Responding to Terms of Reference

a. challenges facing Australian law enforcement agencies arising from new and emerging ICT;
    a. Unable to monitor communications, even after Government shares an early secret Quantum Computer
    b. Unable to unlock encrypted mobile devices and storage
    c. Fast satellite communication outside of national jurisdiction
    d. Unable to easily follow money trail (Cryptocurrency)
    e. Counter Surveillance from Consumer Drones, Number Plate and Facial recognition
    f. Espionage - stealing information from Law Enforcement agencies. Using readily available hacking tools, and social engineering.
b. the **required** ICT capabilities of Australian law enforcement agencies;

[1] iPhones and Android smartphones for instance

    a. Current capabilities are unknown, and therefore new and emerging ICT tools are discussed instead.
    b. Targeted hacking, malware, keylogging and more by Law Enforcement with Warrant, don't apparently impact human rights. However, the most dangerous organised criminals are aware of this, and may limit the use digital devices and find ways to avoid long-term malware infection.
    c. Broad passive data collection and monitoring is a sensitive issue, and unlikely to be sustainable.
    d. Physical practical capabilities are most recommended. However, this is less scalable.
c. engagement by Australian law enforcement agencies in our region;
    a. Not applicable
d. the role and use of the dark web;
    a. This is already widely reported on, and comes under the broad heading of "Communication Encryption"
    b. Communication Encryption and countermeasures are discussed above in section [b]
e. the role and use of encryption, encryption services and encrypted devices; and
    a. Encryption services comes under "Communication Encryption" broadly, specific types are noteworthy but not important when considering countermeasures
    b. Encrypted devices, password protected drives and files, all come under "Storage Encryption".
    c. Both of these matters are addressed in section [b] above
f. other relevant matters
    a. Is mass internet surveillance politically and ethically possible?
        i. For
            1. Protection of the many
            2. Will enemies (who are not ethically bound by voters) eventually have more surveillance infrastructure and know more about citizens than governments (who are accountable)?
        ii. Against
            1. The worst offenders will find ways around it
            2. There is considerable potential for bad individual actors in government to abuse the power of information
            3. Groups who are against it in principle, who will never be convinced otherwise, and can gain public attention quite easily
    b. Further Research and confidential information that is available to some ministers will be useful for decision making
        i. Is asymmetric encryption breaking possible by Governments today secretly? Possibly with a Quantum Computer[2]

Context and Background

- "new and emerging ICT"

[2] See http://blog.alivate.com.au/busted-internet-community-caught-unprepared/

    - Mobile Broadband, moving toward 5G
    - Satellite Broadband in Low-Earth Orbit
    - Simple toolkits, support and marketplaces for hacking - MetaSploit, Forums, Custom Viruses with 24/7 support
    - Communication Encryption - Telegram App, Off-The-Record (a new key each session), One Time Pad (symmetric), and Quantum Encryption (only a small incremental increase in security), VPN, and TOR and I2P
    - Storage Encryption - Mobile device storage encryption, PC hard disk encryption
    - Cryptocurrency - Blockchain, Anonymous Currency
    - Consumer drones - Autonomous, counter surveillance
    - Software Defined Radio (SDR) - Wide range of frequencies, and protocols are accessible, to discover, localise, listen, and transmit. Computing power is increasing which lowers the cost for advanced 3D spatial localisation tools.
    - Open AI - number plates, and facial recognition
    - Post-Quantum Encryption
- There are many vulnerable software and hardware devices, with many known current and exploitable weaknesses
    - Keylogging is the most critical weakness in systems today
        - Most relevant for PC's but also mobile devices
        - This generally requires implanting malware on a device, but many wireless keyboards are not sufficiently encrypted, and keystrokes can be recovered nearby
        - capturing passwords used to encrypt/decrypt stored information
        - capturing typed messages before they are communicated, working
    - Capturing audio and video from Mobile and Desktop devices
        - capturing information (from conversations, and visuals) beyond what is expected to be communicated or stored
    - Radio Frequency Emissions
        - many devices not designed to transmit radio signals, still emit radio noise. This noise can be correlated to information from computer peripherals, computer screens, and even to the extent of information being processed in a CPU, including passwords
- Practical methods for gathering evidence and information, in an encrypted digital world
    - Bug - a sound recording device which must be physically and discretely installed, and recovered.
    - Long Range Listening - for example, it is feasible to watch a potato chips wrapper through a window, and recover audio from the vibrations caused by noise in a building.

About the author

- See https://www.linkedin.com/in/toddhubers/
- Software Engineer
- Bachelor of Business Information Technology (Hons.)