Intruding on Intrusion Software

Cristin Flynn Goodwin
Assistant General Counsel
October 28, 2015

Start with a scenario to identify the problem

What's the problem we're trying to solve?

Assumed scenarios or scope of concern:

- Exploiters of technology may be individuals, groups, criminal enterprises or nation states
- Targeting specific individuals, rather than large groups
- For the purpose of:
  - Surveillance
  - Data extraction / exfiltration
  - Social engineering (including technical modification of system in order to trigger a particular action or response)
- Without the express or implied consent of the target

Leveraging data to solve hard problems and measure success

Leveraging the law

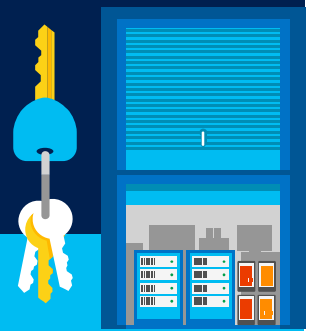
Assumptions about "Why Wassenaar"

- Aimed at private sector / non-government actors only, as governments are not required to obtain licenses
- Seeks to curtail criminal behavior through the creation of export control obligations
  - Assumption that this could create additional enforcement tools for law enforcement?
  - Assumption that national export control regimes will have relevant enforcement regimes to enable deterrence
- Recognizes that nation states will still be able to create, or cause to be created, software for the purposes identified in the "intrusion software" definition
- May or may not be criminal behavior to use this software (as defined) for the intended purpose, despite the export control obligation contemplated by "intrusion software" scope

Options and Ideas

How do we drive to the desired outcomes?

Focus on the *intent* to obtain information about a person, device, system or network



Intent

Focus on the intentional lack of consent as driving the need for a license

Consent

Focus on the extraction of data (or metadata) from a person, device, system or network

Extraction

Cybersecurity and changing global norms


Microsoft