Opportunities for cooperation between the CSIRT and law enforcement for protecting critical infrastructure

CoE Guidelines on LE & ISP cooperation

- Guidelines from 2008
- Adopted in France a few months after. Now translated to 16 languages
- Primarily focused on streamlining the rendering of evidence in criminal cases
- Suggest more broad cooperation outside of specific cases such as discussing Modus Operandi of criminals, crime trends, and improvements of evidence available at ISPs

Protecting critical infrastructure

- Network & Information Security Directive with transposition date in May 2018
  - Establishes national CSIRTs
  - Requires them to work together in a network for cooperation
  - Identify operators of essential services and require incident notification
- 2017 Petya variant attack shows essential services are not easily defined

Understanding technology

- Some technology is well understood (such as the Windows file system), other technologies are not well documented
- Understanding technology can be used to understand available evidence and attack surfaces
- DAD triad (Disclosure, Alteration, Denial) cannot be understood without a technical explanation of for example unauthorized access

Seeing crimes and understanding new threats

- IT infrastructure is entirely privately owned and shielded off. It is so complex that RFCs are no longer what needs to be examined.
- Crimes are likely to have elements committed abroad. CSIRTs already work together to share threat information
- Computer data often have complex distribution. Only the CSIRT can view this data and understand trends and new threats

Evidence collection

- Cloud Act and EU e-evidence instruments for prosecutors to retain investigative powers when evidence is located abroad
- Identifying where it is available, Paul Manaford case where evidence was hidden in 7 iPods seized as well as the iCloud backup of encrypted WhatsApp messages

Questions