Crime and Communication Technology
Paul Ekblom

Ekblom, P (2014). 'Crime and Communication Technology', In W. Donsbach (Ed.) *The International Encyclopedia of Communication,* 2nd Edn. Oxford: Blackwell Publishing.

Crime has a complex, evolving relationship with the communications *function* and communication *technology* (⇨Communication Technology). Crime control involves conventional law enforcement and 'scientific' approaches.

Crime varies in target from property to persons, organizations, and systems; in motive from materialism to sex, revenge and ideology; in complexity from vandalism to people-trafficking. *Fear* of crime independently reduces quality of life, implicating the Media (⇨Crime Reporting; Risk Perception). The *trust* supporting transactions, customarily generated face-to-face, is unavailable from remote communications (⇨E-Commerce).

Communications can be *Misappropriated* (hardware stolen, service fraudulently obtained); or *Mistreated*, including damage via hacking (⇨Hacktivism). *Mishandling* includes improperly obtaining/altering messages. *Misjustification* occurs when pedophiles, through self-selecting newsgroups, assume their activities are widespread (⇨Network Organizations through Communication Technology). *Misbehaviour* includes 'trolling' (aggressive social media messages). Communications *Misused* for crime include deception (phishing); selling stolen goods; coordinating riots; detonating bombs.

Law-enforcement has significant limitations. Preventive approaches promising greater capacity and cost-effectiveness and fewer side-effects include *Situational crime prevention.* This changes immediate environments via perceived risk, effort and reward to influence opportunity and criminals' decisions to offend.

The Conjunction of Criminal Opportunity framework combines situational and offender-based perspectives on causation and prevention; Collins and Mansell (2004:63-4) apply it to cyberspace. It describes causation of criminal events via *offenders* predisposed, motivated and equipped for crime, encountering or engineering *crime situations* with vulnerable targets in conducive environments. Situations may lack crime *preventers* and contain 'crime *promoters*': careless users, say, or those knowingly supplying illicit passwords.

Designers face tradeoffs between security versus cost, convenience, privacy and safety. Making systems simultaneously *user-friendly* whilst *abuser-unfriendly* demands informed creativity, subtlety and competence in technology and *human factors*. Designers of new applications/systems rarely 'think thief': marketing vulnerable products/services generates 'crime harvests', then awkward retrofitted security. Emergent properties of complex systems breed surprise opportunities. *Laws* lag changes in crime (⇨Internet Law and Regulation). *Secure design* frameworks exist (Ekblom 2012).

Preventive *methods* are perishable: crime preventers, in an arms race, must out-*innovate* criminals; and anticipate, researching *offender capabilities*, *horizon-scanning*, building-in *future-proofing* and generating *varied* security measures.

Toleration of crime, widespread in commerce facing high financial/reputational costs of criminal justice involvement, fosters *collective* costs including mistrust. Companies' savings on security externalize costs to users (e.g. exposure to identity theft from insecure services), other citizens and taxpayers. Governments intervene by incentivizing crime prevention, awakening consumer pressures and 'naming and shaming' suppliers.

SEE ALSO: Communication Technology; Crime Reporting; E-Commerce; Hacktivism; Internet Law and Regulation; Media Use and Child Development; Network Organisations through Communication Technology; Risk Perception; Socialisation and the Media; Terrorism and Communication Technology

REFERENCES AND SUGGESTED READINGS

Collins, B., & Mansell, R. (2004). *Cyber Trust and Crime Prevention: A Synthesis of the State-of-the-Art Science Reviews*. London: Department for Business, Innovation and Science.

Ekblom, P. (2012) (ed.). *Design Against Crime: Crime Proofing Everyday Objects.* Boulder, CO: Rienner.

Home Office (2013). *Cyber crime: a review of the evidence.* London: Home Office.

BIO

Paul Ekblom is Professor of Design Against Crime at Central Saint Martins, University of the Arts London; and visiting professor at UCL and Huddersfield Universities. He also writes on crime futures and co-evolution, and has created frameworks for mapping causes of crime and preventive interventions, at www.designagainstcrime.com/web/crimeframeworks.

Lexicon Words: Communication Law and Policy, Technology