The 16th biennial conference of the Society for Philosophy and Technology
Track 3: Converging technologies and risks

Wolter Pieters
Centre for Telematics and Information Technology, University of Twente

Converging technologies and de-perimeterisation: towards risky active insulation

In converging technologies (Roco and Bainbridge, 2003), boundaries between previously separated technologies become permeable. A similar process is also taking place within information technology. In what is called *de-perimeterisation* (Jericho Forum, 2005), the boundaries of the information infrastructures of organisations dissolve. Where previously a firewall was used to separate the untrusted outside from the trusted inside, outsourcing of information management and mobility of employees make it impossible to rely on such a clearly located security perimeter. In this paper, we ask the question to what extent these developments represent a similar underlying shift in design assumptions, and how this relates to risk management (cf. Perrow, 1999). We investigate this question from the perspective of the system theory of Niklas Luhmann (1979, 1988, 2005 [1993]).

In order for technologies to function, they need to "decide" which influences they let in or out. This is what Luhmann calls *causal insulation*. We can distinguish between *passive* and *active* causal insulation. In passive insulation, the insulation is implicitly realised by "common" physical properties. In active insulation, a special mechanism is included in the design that is supposed to take care of the protection. A piece of paper is in principle not accessible, *unless* you have the paper in your hands (the so-called "air gap"). A file on the Internet is in principle accessible, *unless* it is actively protected (e.g. by encryption).

As an example, consider the difference between barcodes and RFID (radio-frequency identification) chips on consumer products. The information in the former can not easily be captured from a distance, since the products mostly reside inside shopping carts and bags. By contrast, the information in RFID chips can be read, *unless* there are protective measures in place. This makes the security of the RFID information dependent on the adequacy of the security protection mechanism. Such differences also apply when boundaries fade with de-perimeterisation and converging technologies: there is a shift from passive causal insulation to active causal insulation due to increased connectivity.

Active protection, in contrast to passive protection, is by definition based on design decisions. This means that, in Luhmann's terminology, the possibility of failure is always one of risk instead of danger: one could have made a different design decision, which is not the case with passive protection by physical separation of technologies. Moreover, how the protection works can no longer be understood without specialist knowledge. It is easier to convince the public that barcodes cannot be read from a distance than to achieve the same result for RFID, even when experts find the protection adequate. This means that trust becomes increasingly important. Instead of unconsciously relying on the physical separation of systems, we have to decide consciously whether we trust a security measure to protect our assets.

Simultaneously, increased connectivity often amounts to a shift from causal insulation based on physical separation to causal insulation based on informational separation, called "non-interference" in computing science (Sabelfeld and Myers, 2003). Whereas a traditional pill relies on chemical properties to release its contents, a digital pill may be steered from outside

the body, requiring again active protection, which is typically based on informational properties rather than physical properties (e.g. authentication and encryption).

When insulation is insufficient, as in the case of de-perimeterisation, an alternative or complementary approach is to detect when a technology is being misused. In information technology, this is called *intrusion detection* (Bolzoni and Etalle, 2008). Based on the similarity between de-perimeterisation and converging technologies, we predict that intrusion detection will increasingly be applied in to converging technologies as well, shifting the design assumptions from protection towards detection. When everything is connected in the information domain (Internet of things), lack of protection may lead to for example digital pills being "hacked". In such a case, pills need to be suspicious about the instructions given to them: if they get a strange sequence of instructions, they may decide not to execute them and generate a warning instead. Moreover, this security mechanism will *itself* rely on information about the use of the device, which also needs to be protected.

Concluding the argument, converging technologies and de-perimeterisation are similar in that both involve in their design assumptions the dissolution of boundaries, a shift from passive to active protection, and a shift from physical to informational insulation. This makes protection both more risky, in the sense of based on design choices, and more subject to specialist knowledge and therefore trust. Because of the shift towards informational insulation, the complementary use of insulation and intrusion detection in computing science will increasingly apply to converging technologies as well.

References

Bolzoni, D. and Etalle, S. (2008) Approaches in Anomaly-based Network Intrusion Detection Systems. In: *Intrusion Detection Systems*. Advances in Information Security 38. Springer Verlag, London, pp. 1-15.

Jericho Forum (2005) *Jericho whitepaper*. Jericho Forum, The Open Group. URL: http://www.opengroup.org/jericho/vision_wp.pdf.

Luhmann, N. (1979) *Trust and power: two works by Niklas Luhmann*. Wiley, Chichester.

Luhmann, N. (1988) Familiarity, confidence, trust: problems and alternatives. In D. Gambetta (ed.), *Trust: Making and breaking of cooperative relations*. Basil Blackwell, Oxford.

Luhmann, N. (2005 [1993]) *Risk: a sociological theory*. Transaction Publishers, New Brunswick.

Perrow, C. (1999) *Normal accidents: living with high-risk technologies*. University Presses of California, Columbia and Princeton.

Roco, M.C. and Bainbridge, W.S. (Eds.) (2003) *Converging Technologies for Improving Human Performance*. NSF-DOC Report, Kluwer, Boston. URL: http://wtec.org/ConvergingTechnologies.

Sabelfeld, A. and Myers, A.C. (2003) Language-based information-flow security. *IEEE Journal on Selected Areas in Communications*, 21(1), pp. 5-19.