Universal electronic systems breakdown

003

FP7 themes	health	agro	ict	nano	energy	environment	transport	ssh	space	security

ERA goals	mobility	infrastructures	rtd institutions	knowledge sharing	joint programming	cooperation

Author(s)	Yanuar NUGROHO (University of Manchester), David CAIN (Regional Technology Centre North), Rafael POPPER, Thordis SVEINSDOTTIR (University of Manchester)
Contributor(s) *UK workshop participants in the ENVIRO-SSH group*	Peter ELLWOOD (Health and Safety Laboratory), Fiona LICKORISH (DEFRA), John REYNOLDS (SAMI consulting), John TURNPENNY (University of East Anglia) and Martin FATUN (Technology Centre), Joe RAVETZ (University of Manchester)
Manifestation	Gradual development
Importance for EU	★ ★ ★ ★ ★
Strategic attention	by 2030 ★ ★ ★ ★ ☆ by 2050 ★ ★ ★ ★ ★
Type of impact	Very negative
Inspired by	Brainstorming session and group discussions in the iKNOW Workshop in Manchester (February 2010)

Potential impacts in Europe

infrastructures	★ ★ ★ ★ ★
people's lives	★ ★ ★ ★ ★
legislation & regulation	★ ★ ★ ★ ☆
economy & business	★ ★ ★ ★ ★
defence & security	★ ★ ★ ★ ★
government & politics	★ ★ ★ ★ ☆
environment & ecosystems	★ ★ ☆ ☆ ☆
science & technology	★ ★ ★ ★ ★

Key words	Vulnerability, sophisticated society, networked society, communication, standards

Negligible ★   Minor ★ ★   Moderate ★ ★ ★   Major ★ ★ ★ ★   Critical ★ ★ ★ ★ ★

Wild card

This wild card (also called "when lights go off") relates to the vulnerability of "advanced" societies, especially those in which information and communication networks are based on a few electronic standards. This has been happening right now with the emergence of standard protocols (i.e. TCP/IP, to the 3G, etc.) which, whilst on the one hand eases the communication processes, on the other hand creates vulnerability. One unexpected event (e.g. a terrorist attack or a sun wave storm) could lead to a global electronic systems breakdown and the advanced technological societies would be hit hard by this as everything we do now is controlled in some way by technology.

Surprises ('wild' scenario features)

That our societies have become networked, thanks to the advancement of electronic and computing devices, has been discussed and theorised since 1960s. The fact that our societies are more and more reliant on a few electronic standard systems and protocols is also known. Standardisation has indeed offered ease and convergence but at the same time poses risks. The question here is how to achieve systems compatibility without standardisation? A universal electronic systems breakdown, however, would not come out of the blue as markets force systems to use cheap, yet vulnerable, components which are most vulnerable to attacks or breakdowns. A systems blackout would disrupt most aspects of our life, as modern societies could be described as one giant interconnected e-system. Networked societies have allowed us to be connected with each other via technological advancement but they have also brought major risks. In the potential event of major electronic data loss (e.g. personal, financial or scientific, to name a few), there would be massive civil unrest. In a particular context such as in cold climate, the impact could be devastating and serious as this wild card will affect the life-support systems like gas, heating, water, and electricity.

Possible interpretations

There are many conditions making this wild card ferocious. But here we will explore three possible interpretations. Firstly, that we rely too much on single systems which are interconnected. The world has now become a giant network. Instead of having many independent (or interdependent) systems, we are relying on and building one massive system which we hope can hold everything. This is highly risky. Secondly, that we do not have alternative/back up source of energy. We may need to provide an independent (mobile) energy generator to anticipate the failure of the main generator either due to attack or natural disaster like sun wave storm. Lastly, that we do not really have a map of the areas of vulnerability. We do not really know what aspects of our societal life are really vulnerable and what can be handled with reasonable planning when things go wrong.

Key actors

Key actors related to this wild card, include:

- **Scanners** or "early warners" such as scientists who monitor the sun's activities; researchers who are developing universal electronic protocol standards.

- **Shapers** (i.e. enablers/inhibitors): governments, regulators, global actors (e.g. TNCs) and energy companies.

- **Stakeholders** positively or negatively impacted: society in general as the wild card will actually impact on all of those whose life depends more and more on the sophistication of technology; energy companies who not only will suffer from losing control to the energy supply but will also face pressures from consumers and regulators; police and the army who has to anticipate riots and violent actions as the wild card directly crashes the existing social order.

Potential impacts

This wildcard will bring about total chaos, as all aspects of our societal life are dependent on the one standardised, electronic network. As result there will be chaos, as nothing works. This chaos will inevitably lead to major civil unrest/crime. With the electronic systems which manage supply-chain of consumer goods, supply for foods is affected – it is running empty very quickly, worsening the impact.

Potential actions

The actions to address this wild card can probably be directed to these two orientations: firstly, to build backup systems to anticipate if the main system is down; and secondly, to build a more resilient society. To achieve this, a number of early actions (pre-wild card) and early reactions (when the wild card occurs) are devised below.

- **Policy actions**

    Early actions: To prepare for this wild card it is necessary that policies, at national or even supra-national level, are in place to ensure the availability of back-up systems, especially for aspects that are critical to human life.

    Early reactions: Once the wild card happens, the immediate action should be to put policies in place to reintroduce more human control.

- **Business actions**

  Early actions: Business has to be made aware of this wild card and business should be open and supportive to incentives for alternative systems, instead of blindly campaigning for standardisations.

  Early reactions: To anticipate the chaos by collaborating with government and non-government groups to ensure that basic needs are provided for. Then, business needs to change its business model, to aim for alternative systems.

- **Research actions**

  Early actions: Research needs to aim for testing the resilience of back-up systems; to identify most critical vulnerability; to build knowledge bank of low-tech alternatives; to research decentralised systems and incentives; and to study social attitudes to risk and technology dependency – how to overcome resilience and bottom-up organisation for recovery

  Early reactions: To research the resettling of society in the aftermath of massive chaos.

Weak signals

What can indicate that the wildcard is happening? Some signals are identified here. Among others, they are: increasing frequency of interference effect; greater reliance on standard systems; no backup systems – or even if there are, these also depend on the same network. Other indicators are if more communities engage in electrical criminal activity while at the same time we experience a greater reliance on harmonised systems and that machines become more 'intelligent' than humans and we, humans, lose control. This can be easily spotted as we come to rely more on computers in everyday life. Another signal, which links to the natural cause to this wild card is that historical data shows that a sun wave storm happened sometime in the past (17th century?) and that certainly will happen again, only we do not know when.

Recommended research

Thematic area(s)

ICT, environment, energy, social sciences and humanities, and security

Research topic

Societal response to potential blackout of electronic systems.

Contemporary society relies on a communication network, which is based on one electronic standard system. Further standardisation such as TCP/IP and 3G which on one hand ease communication processes on the other hand leads to potential security vulnerability. Increasing reliance on computer systems/networks and increase of computer based crime furthermore increases the vulnerability of societal infrastructures, should a natural disaster or acts of terrorism disable communication and energy systems.

Objective

Research could focus on examining the nature of societal reliance on standardised systems. Research could focus on developing backup systems that could be used in the event of a current system breakdown. Research could identify areas of vulnerability (e.g. security measures at major power plants, likelihood of terrorist attacks) Research could furthermore use foresight methodologies to examine how society could be prepared for alternative ways of living, should a system breakdown occur.

Expected impact

Research should aim to a) inform the development of an alternative energy and communication system; b) devise strategies for crisis response across Europe; c) inform relevant policy, legislation and regulation across EU; d) inform business enterprise and innovation in this field; e) revise existing policies promoting standardisation; f) explore alternative ways of achieving systems compatibility and interconnectedness.

Importance for Europe

Threat to energy safety is an important grand challenge for Europe and grand scale disruption to the energy system could have unforeseen consequences for all levels of society. Finding ways of securing energy flow throughout Europe is vital and innovation in this field is important. Joint regulation is also necessary and EU needs to take initiative to formulate a response in the event of threats to food security. EU policy could then provide blueprint for any policy response from the governments of member states.