IS OUR E-WORLD SAFE? …. STRUCTURAL THREATS

Jaroslav Pejcoch[1]
T-SOFT
Czech Republic

Keywords

e-government, e-business, e-banking, critical infrastructure, risk management.

Abstract

There is more and more e-things in our Word. The infrastructure, which is invisible most of a time, assures quality of our lives and we keep an eye on it, preserving its safety and continuity as we know it represents a sensitive point, which, attacked, might cause us serious problems. We are protecting our infrastructure against natural and industrial disasters, again terrorists and other bad guys.
But there is one more factor – where is the threshold, beyond which the infrastructure might get unstable and collapse? Is there still an opportunity to build nicely structured large systems, well planned for many years or are we facing more to the emerging behavior and supersystems? What are the roles of governments, academic and industry in this situation?

e-world

There has been a growing list of e-somethings all around us in the last years. For example e-business, e-health, e-learning, e-banking, e-books, e-tickets, e-mail, e-government, e-gallery, e-science, e-commerce, e-newsletter, e-passport, e-money, …..

We are more and more dependent on services supported by Information and Communication Technologies (ICT). Such a technologies stand behind almost all systems and devices we are using now and we are dependent on. They control the business finances, logistics and help to interconnect groups of people and support the worldwide virtual teams. In fact, the globalization would hardly be so massive without ICT.

The whole world is getting more complex and interdependent and there is a situation, where we have to add to the standard risks taxonomy (War, Natural, Industrial and Other intentional as terrorism) one more item: Structural.

The systems and especially the ICT part of them are improving and the performance of hardware components is rising. Overall meaning is being accepted that the systems are going to have higher level of artificial intelligence. We should ask ourselves a questions:

- Do we trust them?
- Can we control them forever?
- Can they be misused?

There are some interesting factors, connected with the current situation in the systems development. We may characterize them as “permanent juggling”, “emergent behaviour” and

[1] T-SOFT a.s.; Novodvorska 1010/14; 142 21 Praha, CZ, T: +420 261710561, E: pejcoch@tsoft.cz

"flying concrete building technology". It seems sort of strange on the first glance, but let's look to them more closely:

Weaknesses of the modern society – permanent juggling

Due to the growing complexity of the business and the infrastructure, our world could remind more and more a juggling artist

The perfect orchestration of his hands and various things flying in the air is really impressive and if he is skilled enough or has some colleagues or technology, he may add additional items to juggle or inter-juggle with a growing glance.

But this spectacular show has one very important problem inbuilt. Imagine switching off the light… or holding one of his hands for a while …

The nicely performing system would fall down, all the bells and whistles disappear and everything what depended on its movement would stop.The way back to might be long and painful or even impossible – the new synergy could look completely different.

What is important on the juggling … there is a permanent need to invest energy and maintain control over the whole interrelated system. The failure of a part leads to the collapse of the whole.

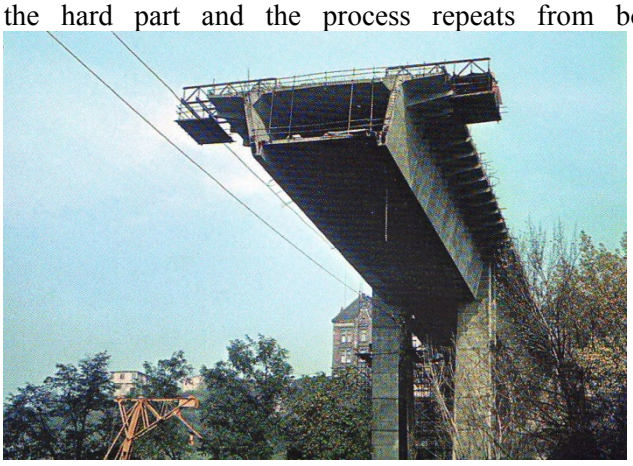
We may identify some parallels in our technology-based and globalized life of a permanent juggling, which cannot be interrupted without substantial problems:

- Cellular networks
- Internet
- Banking system, credit cards
- Logistics
- Energy supply
- …

All of them we need to maintain our standard of life – but more, it seems we could not live further without them.

Flying concrete building

There is a method in the civil engineering, which is used to build bridges over deep valleys effectively. There are bases built on both sides of the valley and the mould is placed at the end, the concrete and steel rods put in and let harden. Then, the mould is pushed forward over the hard part and the process repeats from both sides until they meet and join.



The trick is that a ready part can be used to transport a material for the next increment.

In the area of information systems building we may see in the last time also a shift from the classical waterfall model, where at first "everything was analyzed" then "everything was designed", then "everything was implemented" and ….. in many cases it succeeded.

There is another situation nowadays – there are no more singular systems, which would be able to create this way, there is need to interoperate with many yet unknown systems and react to the requests which are not present at the beginning of the project. The incremental way of building systems, taking into account a limited set of starting requirements is more and more typical. The methodologies are being adapted to this new situation, methods called "agile programming" are used to speed up the delivery of a functionality, not practically encompassing the problem in its full complexity.

But the results are here, parts of the systems could be used even that the end (if something like this has a sense) is still far away.

We may also identify a negative of this phenomenon … there are particular optimizations and hidden interdependencies, which might be never discovered.

Emergent behaviour

Another phenomenon, which takes part in our complex e-world is the Emergent behaviour. Based on several simple rules and multiple agents, the objects as a fish shoal, termitarium or anthill appear as pretty organized large systems. The stock exchange is of the same nature.

Such systems might appear very stable and self-regulated, but it is truth only as far as the communication works fine and the elements are compliant to the system. If we induce some false signals, the whole system might collapse.

Interdependencies and Critical Infrastructure

We have to take into account the phenomena described above when contemplating about the critical infrastructure. The physical, informational, logical and geographical interdependencies of its subsystems the way how they are build and operated and the need to keep the whole infrastructure up and running 24 hours x 7days in the week lead to **Emerging Super systems**, which are not intentionally created by anybody, but they *just are there*.

The problem is that due to unknown nature of such super systems we cannot precisely predict what might happen, what might be the consequences and how to mitigate that. Everything is being permanently "under construction" and working as a fish shoal.

The vulnerability of our critical infrastructure is surprisingly increasing with the successful projects and those systems which are neatly structured, interoperable and working smoothly and efficiently. Such a successful systems are gaining our trust, increase our dependency on their functioning and weaken our cautiousness.

The neat and well documented structure and interoperability bring the threat of easier attack by unfriendly subject and also the threat of massive escalation of potential crisis situation. We may see examples of misuse the SCADA control systems over the internet.

Globalisation and security

Having outlined the environment, we may look to the globalisation playground. It is evident, that not only global advantages are here, but also some global threats. The interdependent and "juggled" infrastructure might be attacked by intention. But it also may collapse just by insufficiency in the design (we know that many things were not designed … they just happened) or the feature of the emerged structure, triggered by current setup and situation.

It is also evident that there are contradictory objectives in the society, which might misbalance the stability of the infrastructure. For example in a crisis situation – in the power supply area - the general need would be to supply the energy and help the consumers, while at the producer's side it is evident, that they have to protect their own resources against possible damage by the overload.

In the resources management area there are competing aids of political or humanitarian order and standard business rules. Those facts, if not treated as globally as the global crisis might happen, could lead to the weakness of the infrastructure and its internal crash.

We also might find that utilizing the standards and homogeneous operating environment is on one side very effective and positive factor, but the similarity leads to more vulnerable systems than the heterogeneous and not very smoothly collaborating systems.

A special role plays a security. From the nightmare for the former users and IT managers it became a new possibility – **the enabler**. Only when we assure a proper security measures, we may "let our workers climb to the flying mould".

The proper care of security helps us also to fight the consequences of successful projects. This looks as a contradictory, but we have to bear in mind, that every successful project decreases our level of vigilance, increases our trust to something we just see the outer face of it and do not understand how easily we could be manipulated. So the proper security features are a key factor for further development and protection against structural threats.

Roles of Government, Academics and Industry

Having written all of those things about structural threats and potential collapse of our juggled world, we may specify a distinct roles of government, academics and industry to defend against something we might call "falling into maelstroem" of infrastructure boom.

The Governments have a main role to outline the playground,.define rules and build the preparedness to the potential crisis situation. The legislation role might be very critical in establishment of a proper balance between local and global aims with respect to security.

The Academics is well suited to investigate and watch the complex system environment, simulate the possible scenarios and keep us off the maelstroem.

The Industry task is to keep the progress and maintain the quality of systems being built, incorporating the adequate security features at each level of system.

Conclusion

On the example of three phenomena linked to our current situation in using advanced ICT technologies to build the e-based world (flying concrete, emergent behavior, supersystems), we described the potential of Structural threat in addition to the current threats used for global risk analysis.

Such a threat has to be taken into account in the further development - the way that the industrial society goes to. There seems to be no alternative to this development, unless we return back to low-energy local way of life. The juggled infrastructure can help us to move a thread-up on the spiral, even than the current energy resources would be exhausted. It can help us to produce and maintain advanced technologies needed for sustainable life at the conditions we are used to live. We have to be careful of the fact that in such an infrastructure arise tensions as in the tectonic environment, which threatens to bring an earthquake.

To avoid the total collapse of a permanently juggled and growing infrastructure, proper attention has to be paid at the government or legislation levels to the proper setting up of rules to optimize the behavior of various subjects at the proper level (avoiding business-justified local weakness of the infrastructure). Also to encourage and support the research of the

possible causes and consequences of structural threats and to adequately equip each part (or potential part) of critical infrastructure by security features, which would support the protection against intentional attack and also minimize the possibility of escalation of emergency situation induced by any cause, even spontaneously – due to the complicated structure itself.

References

Cordesman, A. H., Cordesman, J. G., Center for Strategic and International Studies (Washington, & NetLibrary, I. 2002. *Cyber-threats, information warfare, and critical infrastructure protection
defending the U.S. homeland*. Westport, Conn: Praeger.

Dessing, J. C., Daffertshofer, A., Peper, C. E., & Beek, P. J. 2007. Pattern stability and error correction during in-phase and antiphase four-ball juggling. ***J.Mot.Behav.***, 39(5): 433-446.

Ezell, B. C. 2007. Infrastructure Vulnerability Assessment Model (I-VAM). ***Risk Anal.***, 27(3): 571-583.

Gheorghe, A. V. & NetLibrary, I. 2006. *Critical infrastructures at risk
securing the European electric power system*. Dordrecht: Springer.

Goetz, E., Shenoi, S., IFIP Working Group, & ebrary, I. 2008. *Critical infrastructure protection*. New York: Springer.

Kopacek, P., International Federation of Automatic Control, & ScienceDirect (Online service) 2006. Improving stability in developing nations through automation 2006
a proceedings volume from the IFAC Conference on Supplemental Ways for Improving International Stability through Automation ISA '06, 15-17 June 2006, Prishtina, Kosovo..

Kreimer, A., Arnold, M., Carlin, A., & NetLibrary, I. 2003. *Building safer cities
the future of disaster risk*. Washington, D.C: World Bank.

McDermott, P. 2007. *Who needs to know?
the state of public access to federal government information*. Lanham, Md: Bernan Press.

Sullivant, J. 2007. Strategies for protecting national critical infrastructure assets
a focus on problem-solving..

United States, President's Critical Infrastructure Protection Board, United States, & Dept.of Energy 2002. *21 steps to improve cyber security of SCADA networks*. Washington, D.C: President's Critical Infrastructure Protection Board.

United States, Congress, House, Committee on Government Reform, & Subcommittee on Technology, I. P. I. R. a. t. C. 2004. *Telecommunications and SCADA
secure links or open portals to the security of our nation's critical infrastructure? : hearing before the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census of the Committee on Government Reform, House of Representatives, One Hundred Eighth Congress, second session, March 30, 2004*. Washington: U.S. G.P.O.

United States, Congress, House, Select Committee on Homeland Security, Subcommittee on Cybersecurity, S. a. R. a. D., United States, Congress, House, Select Committee on Homeland Security, & Subcommittee on Infrastructure and Border Security 2005. *Implications of power blackouts for the nation's cybersecurity and critical infrastructure protection
joint hearing of the Subcommittee on Cybersecurity, Science, and Research and Development*

and the Subcommittee on Infrastructure and Border Security of the Select Committee on Homeland Security, House of Representatives, One Hundred Eighth Congress, first session, September 4, 2003 and September 23, 2003. Washington: U.S. G.P.O.

United States, Congress, House, Committee on Energy and Commerce, & Subcommittee on Telecommunications and the Internet 2006. *Cybersecurity protecting America's critical infrastructure, economy, and consumers : hearing before the Subcommittee on Telecommunications and the Internet of the Committee on Energy and Commerce, House of Representatives, One Hundred Ninth Congress, second session, September 13, 2006*. Washington: U.S. G.P.O.

Wolfe, J. M., Place, S. S., & Horowitz, T. S. 2007. Multiple object juggling: changing what is tracked during extended multiple object tracking. ***Psychon.Bull.Rev.***, 14(2): 344-349.

Author

Jaroslav Pejcoch isTIEMS International Director for Scientific Programme.
President and co-founder of T-SOFT Company (Crisis management, Interoperability, Security - 70 people). Before T-SOFT worked at the Electronic Research institute Tesla VÚST as Director of IT Division (120 people). Founding member of the AFCEA Czech Chapter, member of the Board of Directors. Member of the Czech National Committee of ISDR. Member of the Presidium of the Czech Association of Crisis Managers. 1975 – Czech Technical University – Faculty of electronic. Publication activities in areas of computer graphics, computer user interfaces, information and communication technologies, information logistic, systems for protection of citizens and environment, interoperability of systems, crisis management, critical infrastructure protection. Married, 4 children. Hobbies: Music (active piano player), Mountaineering, Photography.
www.t-soft.eu, pejcoch@tsoft.cz