proceedings

MDPI

Proceedings

Social Engineering—The Hidden Control †

Edina Albininé Budavári * and Zoltán Rajnai

Doctoral School on Safety and Security Sciences, Obuda University, 1034 Budapest, Hungary; rajnai.zoltan@bgk.uni-obuda.hu

* Correspondence: budavari.edina@phd.uni-obuda.hu

† Presented at the 14th International Conference on Interdisciplinarity in Engineering—INTER-ENG 2020, Târgu Mureș, Romania, 8–9 October 2020.

Published: 31 December 2020

Abstract: The former energy-wasting lifestyles of developed societies can no longer be sustained. In our age, efficiency is the key to continued sustainability. Increasing efficiency requires the use of infocommunication systems and their regulation. Regulatory modeling is based on the cybernetic loops model. The systems are not closed, so they are constantly suffering from environmental disturbances. External interference can also come from a human resource that covertly exploits the technological and psychic elements of the system to achieve its own goals. Social engineering is also such an intervention. The aims of the present study are to draw a parallel between cybernetic loops and social engineering, then to define social engineering on the cybernetic base.

Keywords: social engineering; cybernetic loop; hidden control; definition

1. Introduction

Throughout history, with the development of industry, humanity's energy needs have steadily increased. At the same time, humanity has scattered on the surface of Earth. The resources of the planet are finite. There is less opportunity for an energy-wasting lifestyle as the resources of the environment are depleted. Improving the quality of life requires long-term sustainability [1,2]. In terms of production, the new paradigm of advanced industry, Industry 4.0, targets environmental sustainability [3–5]. In terms of consumption, sustainability is also reflected in the design of the Smart City model [3,6–8]. The vital basis for all this is the operation of appropriate information technology systems [9,10] and their control [11,12]. The new generations of humanity must already grow up according to these principles. These principles need to be incorporated into the legal framework [13] and into the educational materials that define the daily approach [14–18].

One way to increase system efficiency is to increase the efficiency of system management. The implementation of the system control includes the monitoring and event management of the system [19–23]. These activities are consistent with the process model of cybernetic loops. The operation of real and virtual systems is always disturbed by external sources. External interference can also come from a human resource that covertly exploits the technology and psychic elements of the system to achieve its own goals.

The purpose of the intentional regulatory elements included in the model of the cybernetic loop is to implement the operation of the system over time. This also ensures the sustainability of the system. The purpose of social engineering is to interfere with the system in a covert way [24]. The intervention from a source unknown to the system operators is for an external purpose. This intervention serves its own purpose, not the sustainability of the system. The process leading to intervention is similar in both cases, which is why it is worth examining the parallels between the two methods.

2. Methods

The examination of social engineering can also be done with the applied methods and the used resources' technological and quality requirements groupings. In such an examination, distinction can be made between techniques that exploit people and those that exploit technical possibilities. Further distinction can be made according to whether these are techniques used in real physical space or techniques used in the virtual world. The techniques can be applied in a complementary manner. Furthermore, in terms of resource utilization, impacts can work in a direct or indirect way [24].

The control theory cybernetic loop model is based on modeling the control process. Thus, the parallelism between the process of social engineering and the model of the cybernetic loop is worth studying from the aspect of the cybernetic loop. The groupings mentioned above are not suitable for this. For this reason, a new approach must be taken. An approach can base on process modeling.

To achieve this,

1. It is worth simplifying the cybernetic loop model:
    a. The processes that interact with and independently of the system must be identified;
    b. The direction of signal flow for interacting with the system must be identified;
2. The processes of social engineering should be generalized from the aspect of the resulting simplified model:
    a. The processes that interact with and independently of the system must be identified;
    b. The social engineering toolkit needs to be typified in terms of interactivity;
    c. The direction of signal flow for interacting with the system must be identified;
3. The process model of social engineering should be synthesized according to the model of the cybernetic loop.

This approach provides an opportunity to examine the parallels between the two models and to draw further conclusions.

3. Results

The steps identified for the methodology could be performed as follows:

- Based on the operational process of the cybernetic loop, the operational phases of social engineering can be identified;
- Based on the elements of the model of cybernetic loop, the toolbox of social engineering can be grouped and typified;
- Using the typified toolkit, the direction of signal flow could be determined;
- The process model of social engineering could be synthesized based on the model of the cybernetic loop.

The methodology used for the new theoretical approach made it possible to create a process model of social engineering. As the process model was synthesized on the basis of the cybernetic loop model, it was also suitable for standardization and further conclusions. The created model and the results achieved by its use are as follows:

- The logical process of social engineering can be paralleled with the process of regulation;
- Based on the parallelism, social engineering is a manifestation of regulation;
- As social engineering can be understood as a manifestation of regulation, it can be incorporated into the model of the cybernetic loop, which results in a unified process model;
- Based on the unified process model, a cybernetic definition of social engineering can be given.

4. Discussion

The examination of the tools and process of social engineering from the cybernetic aspect included in the study reflects a new unique system of criteria. In this new system of criteria, the examination of the set of tools, intervention process and actors of social engineering is the same as the main elements of the information security approach system [3,5,7,8,25–27].

In accordance with the methodology of the examination, after the simplification of the scope of regulation, the processes of social engineering are examined and the set of tools is typified. After this, the parallelism of the two process models can be detected. As a further consequence, a combined model of the cybernetic loop and social engineering can be compiled.

4.1. Cybernetic Loop

The regulation is a closed, continuous control process among the process models that can be used to control the system in control theory. The basic element of control modeling is the cybernetic loop model. This model represents the process of intervention in the system [5]. Its general structure contains a part-process regulated in the system. Negative feedback is associated with that part process, which realizes the control. The model also includes the effect of environmental disturbance. According to its operation, the control system receives feedback information about the state of the system from the starting point. Comparing the obtained state with the desired state, the control system produces the intervention that is at the end of the feedback.

The simplified general model of the cybernetic loop is shown in Figure 1.

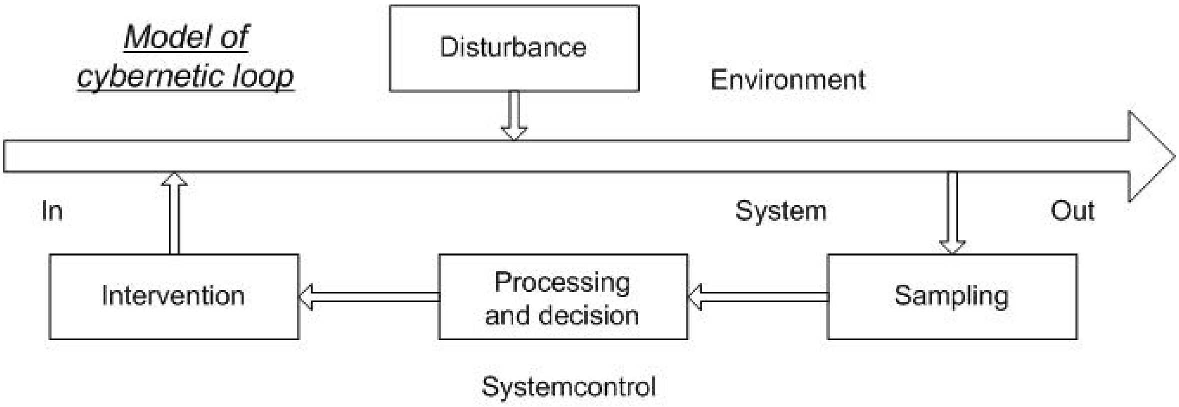

Figure 1. Simplified general model of cybernetic loop.

4.2. Social Engineering

The goal of social engineering is to utilize system resources for system-independent external purposes in a way that is unobtrusive to system management. Throughout history, many techniques have emerged to accomplish this. According to the methodology included in the study, the techniques of social engineering should be typified on the model of the sub-processes included in the simplified model of the cybernetic loop. In this way, the basis of grouping is the interactivity with the system and its orientation.

Based on the grouping of information acquisition, processing and decision, the intervention can be as follows:

- Techniques for obtaining information: impersonation, shoulder surfing, dumpster diving, piggybacking, tailgating, scam, phishing, baiting, and OSINT (Open-source intelligence);
- As the method of data processing and decision making is completely independent of the implementation of the system, the same central technologies can be used to control system and social engineering. However, in the case of the use of distributed technologies, there is a high probability that the hidden state will disappear. Thus, manual correlation search technologies,

data warehousing solutions, the use of artificial intelligence, and central decision systems can also be mentioned here;

- Intervention techniques: asking for help, providing help, taking advantage of reciprocity, impersonation, piggybacking, tailgating, scam, phishing, DNS-based (Domain Name System based) attacks, whaling-type attacks, and baiting.

Some of the techniques listed can be used both to obtain the necessary information and to carry out the intervention. In such cases, the technique usually provides coverage in the system.

4.3. The Paralell

The techniques in the palette of social engineering can be typified on the pattern of sub-processes in the simplified model of the cybernetic loop. Based on this, the parallel can be established. Sampling is a sub-process in the cybernetic loop model that aims to extract information from the system. This is equivalent of this information acquisition in social engineering. As information processing and decision making are present in both cases as separate subsystem processes in parallel with the operation of the system, the parallel of these is self-evident. In addition, these sub-processes require abstract processing, so both models have nearly the same palette. Finally, in both cases, the sub-processes implementing the intervention can be identified. The difference between the two models is that in the case of social engineering, the feedback of control is located outside the system and hidden. This is shown in Figure 2.

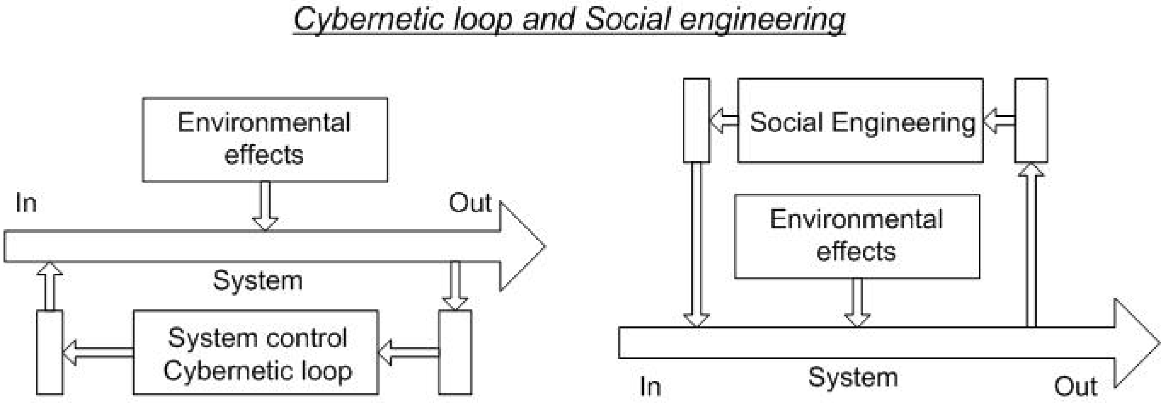

Figure 2. The parallel between the cybernetic loop and the operating scheme of social engineering.

4.4. Model and Definition

As the parallel can be created between the two models, social engineering can be seen as a hidden external control of the system. The model and this recognition allow for a cybernetic definition of social engineering. Another emerging option is to merge the operating scheme of the cybernetic loop and social engineering. This is shown in Figure 3.

According to the above, the definition could be as follows: social engineering is the hidden external control of a system that seeks to exploit system resources to achieve its own goals.

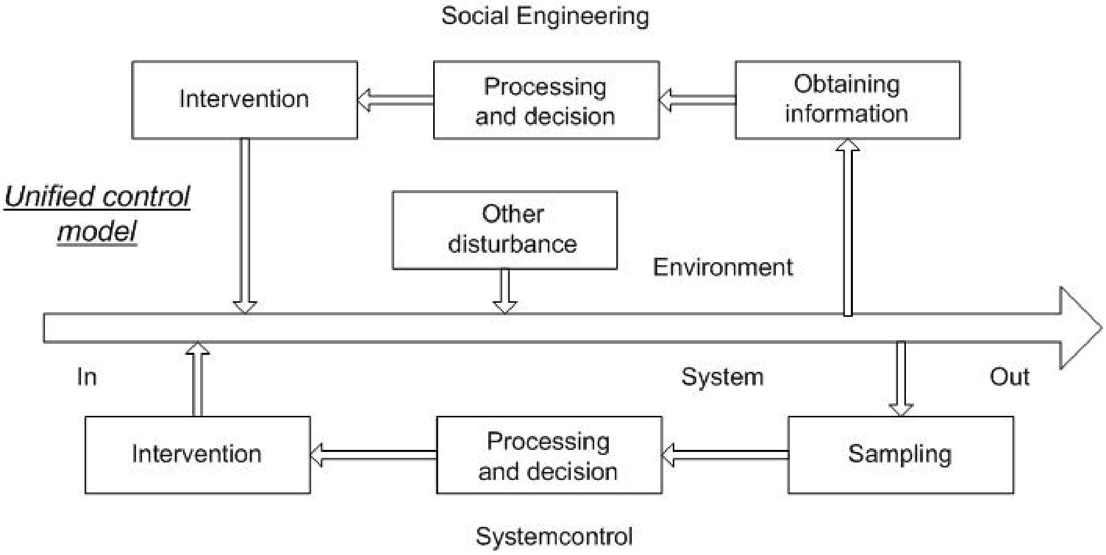

Figure 3. Unified model of cybernetic loop and social engineering.

5. Conclusions

In connection with industrial production, there is a need to cover the entire consumer spectrum of civilization. The industrial products appear in all walks of life. The process of population on our planet requires increasingly efficient use of energy [1,2]. This requirement appeared in all aspects of production. Automation helps increase efficiency. For this reason, the application of advanced infocommunication systems [9,10] is essential for the implementation of the next generation stage of the industry [3–5].

Increasing the management efficiency of the system also increases the efficiency of the operation of the system. The effectiveness of control is determined, among other things, by the application of appropriate cyber regulation. The purpose of this regulation is to ensure the adaptation of the system to external influences [11,12,19–23]. The social engineering is one of the external influences from human resources. This effect takes advantage of the system for an external purpose independent of the system and it is not for the sustainability of the system [24].

The basic element of control modeling is the cybernetic loop of the control theory. This study demonstrated a parallel between the cybernetic loop model and the social engineering process with a new approach. Based on this parallel, it can be stated that social engineering can be considered as a hidden version of cybernetic loop methods. The modeling of the processes ensured the creation of a combined model of the cybernetic loop and social engineering. The unified model, goals and methods made it possible to define social engineering in a cybernetic aspect.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Albini, A.; Rajnai, Z. Modeling general energy balance of systems. *Procedia Manuf.* **2019**, *32*, 374–379. [CrossRef]
2. Kasac, J.; Stefancic, H.; Stepanic, J. Comparison of social and physical free energies on a toy model. *Phys. Rev. E* **2004**, *70*, 016117. [CrossRef]
3. Kiss, M.; Breda, G.; Muha, L. Information security aspects of Industry 4.0. *Procedia Manuf.* **2019**, *32*, 848–855. [CrossRef]
4. Tokody, D. Digitising the European industry—Holonic systems approach. *Procedia Manuf.* **2018**, *22*, 1015–1022. [CrossRef]
5. Kiss, M.; Muha, L. The Cybersecurity Capability Aspects of Smart Government and Industry 4.0 Programmes. *Interdiscip. Descr. Complex Syst.* **2018**, *16*, 313–319. [CrossRef]

6. Tokody, D.; Schuszter, G.; Papp, J. Study of How to Implement an Intelligent Railway System in Hungary. In Proceedings of the IEEE 13th International Symposium on Intelligent Systems and Informatics (SISY 2015), Subotica, Serbia, 17–19 September 2015.
7. Szabó, Z. The effects of globalization and cyber security on smart cities. *Interdiscip. Descr. Complex Syst.* **2019**, *17*, 503–510. [CrossRef]
8. Pető, R. Security of Smart City. *Interdiscip. Descr. Complex Syst.* **2019**, *17*, 13–19. [CrossRef]
9. Albini, A.; Rajnai, Z. General Architecture of Cloud. *Procedia Manuf.* **2018**, *22*, 485–490. [CrossRef]
10. Albini, A.; Tokody, D.; Rajnai, Z. Theoretical Study of Cloud Technologies. *Interdiscip. Descr. Complex Syst.* **2019**, *17*, 511–519. [CrossRef]
11. Mester, G. Obstacle Avoidance and Velocity Control of Mobile Robots. In Proceedings of the 6th International Symposium on Intelligent Systems and Informatics (SISY 2008), Subotica, Serbia, 26–27 September 2008.
12. Mester, G.; Rodic, A. Sensor-Based Intelligent Mobile Robot Navigation in Unknown Environments. *Int. J. Electr. Comput. Eng. Syst.* **2010**, *2*, 1–8.
13. Kovács, Z. Cloud Security in Terms of the Law Enforcement Agencies. *Hadmérnök* **2012**, *7*, 144–156.
14. Rodic, A.; Jovanovic, M.; Popic, S.; Mester, G. Scalable Experimental Platform for Research, Development and Testing of Networked Robotic Systems in Informationally Structured Environments. In Proceedings of the 2011 IEEE Workshop on Robotic Intelligence in Informationally Structured Space, Paris, France, 11–15 April 2011.
15. Mester, G. Rankings Scientists, Journals and Countries Using h-index. *Interdiscip. Descr. Complex Syst.* **2016**, *14*, 1–9. [CrossRef]
16. Dobrilovic, D.; Odadzic, B. Virtualization Technology as a Tool for Teaching Computer Networks. *Int. J. Educ. Pedagog. Sci.* **2008**, *13*, 41–45.
17. Mester, G. Academic Ranking of World Universities 2009/2010. *IPSI J. Trans. Internet Res.* **2011**, *7*, 44–47.
18. Szabó, A.; Szucs, E.; Berek, T. Illustrating Training Opportunities Related to Manpower Facility Protection through the Example of Máv Co. *Interdiscip. Descr. Complex Syst.* **2018**, *16*, 320–326. [CrossRef]
19. Mester, G.; Pletl, S.; Nemes, A.; Mester, T. Structure Optimization of Fuzzy Control Systems by Multi-Population Genetic Algorithm. In Proceedings of the 6th European Congress on Intelligent Techniques and Soft Computing (EUFIT '98), Aachen, Germany, 7–10 September 1998; pp. 450–456.
20. Mester, G.; Rodic, A. Simulation of Quad-rotor Flight Dynamics for the Analysis of Control, Spatial Navigation and Obstacle Avoidance. In Proceedings of the 3rd International Workshop on Advanced Computational Intelligence and Intelligent Informatics (IWACIII 2013), Shanghai, China, 18–21 October 2013; pp. 1–4.
21. Albini, A.; Mester, G.; Iantovics, B.L. Unified Aspect Search Algorithm. *Interdiscip. Descr. Complex Syst.* **2019**, *17*, 20–25. [CrossRef]
22. Zamfirescu, C.B.; Duta, L.; Iantovics, L.B. The Cognitive Complexity in Modelling the Group Decision Process. *Brain Broad Res. Artif. Intell. Neurosci.* **2010**, *1*, 69–79.
23. Mester, G.; Pletl, S.; Pajor, G.; Basic, D. Adaptive Control of Rigid-Link Flexible-Joint Robots. In Proceedings of the 3rd International Workshop of Advanced Motion Control, Berkeley, CA, USA, 20–23 March 1994; pp. 593–602.
24. Albininé Budavári, E.; Rajnai, Z. The Role of Additional Information in Obtaining information. *Interdiscip. Descr. Complex Syst.* **2019**, *17*, 438–443. [CrossRef]
25. Hell, P.M.; Varga, P.J. Drone systems for factory security and surveillance. *Interdiscip. Descr. Complex Syst.* **2019**, *17*, 458–467. [CrossRef]
26. Shatnawi, M.M. Applying Information Security Risk Management Standards Process for Automated Vehicles. *Bánki Rep.* **2019**, *2*, 70–74.
27. Tokody, D.; Flammini, F. Smart Systems for the Protection of Individuals. *Key Eng. Mater.* **2017**, *755*, 190–197. [CrossRef]

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.