

# STRATEGIC AMBIGUITY OF THE TERM CRITICAL INFRASTRUCTURE

**Teodora Ivanuša**

*Ministry of Defence, Slovenian Armed Forces, Slovenia*

**Matjaž Mulej**

*University of Maribor, Faculty of Economics and Business, Slovenia*

**Key words:** critical infrastructure, strategic definition, CBRN devices, ambiguity, systemic thinking

## **Abstract**

One of the enhanced points of the executive summary of EU Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Doctrine (CBRN EOD) for Multinational Operations is “to protect personnel, materiel, infrastructures and environment and to maintain or restore operational capabilities...” Indeed, because of CBRN EOD risk potential (as a rule large danger areas with the possibility of extremely negative effects on the mission, population, infrastructure and environment due to contamination) CBRN EOD tasks are never autonomous tasks; allocation of responsibilities is a necessary applied national routine in which the essential imperative is to avoid individual unauthorized action!

It is complex enough to require systemic thinking, which enhances interdisciplinary creative co-operation, like the Dialectical Systems Theory does more than the others in Encyclopaedia.

In the light of nowadays threats (i.e. CBRN Devices) that differ rapidly and nearly on a daily basis, the term critical infrastructure calls for a detailed reconsideration. The critical infrastructures are more or less determined, representing mutual and essential principles for the command and control and the execution of multinational CBRN EOD operations. However, some professional remarks will be given according to ambiguity of the definition of the critical infrastructures according to natural or intentional outbreak of the highly contagious diseases. Proper planning often prevents poor performance, therefore, threat analysis, high readiness, tasking, coordination and prioritisation remains the major factors when immediate strategic definition of a critical structure must be appointed. This is why systemic thinking is crucial.

## **Introduction**

It cannot be overlooked that the Republic of Slovenia as EU (European Union) and NATO (North Atlantic Treaty Organization) member possesses the nuclear power plant, which is one of the commonly recognized critical infrastructures. In addition, Slovenia is surrounded with 50 other power plants with 109 reactors; 32 of these are within a radius of 500 km from Slovenia (1, 2). Plead for constant existing nuclear threat is anticipated and represents one of the central strategic points. There is no doubt that nuclear power plant and other common critical infrastructures are issues of a highest national strategic framework.

Critical infrastructure is defined and there are no doubts and no reasons for scientific and professional scepticism. Alliance critical energy is assumed to be delivered from the Alliance energy supply structure based on four forms of energy. Detailed description of these four forms of energy is hopefully completely unnecessary. All threats are focused on energy security, which is a serious tasking complexity (3, 4, 5). The facilities, which are employed in the production, transfer means or

storage and processing energy, would have a debilitating impact on Allies security and/or economy, if incapacitated or destroyed. The chance or probability of conventional or asymmetric attacks that could lead to indirect or even deliberate disruption of critical energy flows in a way that would be highly prejudicial to Allied security and economic stability, includes any risk of attack or disruption by hostile forces or by terrorists (6, 7). NATO might add defining those areas to safeguard the security interests of the Allies and assist national and international efforts. It is of immense importance that EDA (European Defence Agency) and its CBRN EOD Project Team offers plead able Doctrine (8) focused on the operational level providing a feasible approach on the operational requirements. In addition, giving the nature, it is important that EU Member States verify their coherence with similar NATO concepts to ensure full compatibility. It seems that national, regional and international interoperability and “know how” are no longer the adjective issues.

The term critical infrastructure and consecutive strategic documents are circulating around four forms of energy. Vandals, saboteurs, criminals, physical attacks, natural disasters, and misfortune (human error) are therefore perfectly manageable. The mitigation options are well known:

- Intelligence fusion and sharing;
- Projecting stability;
- Advanced EU – NATO and regional cooperation;
- Support to the protection of national critical infrastructures;
- Surveillance and protection of ungoverned spaces (i.e. International waters): from “point” defence to “area” defence;
- Counterterrorism;
- Consequence management;
- Military cooperation.

One of the enhanced points of the executive summary of EU Chemical Biological Radiological Nuclear Explosive Ordnance Disposal Doctrine (CBRN EOD) for Multinational Operations is “to protect personnel, materiel, infrastructures and environment and to maintain or restore operational capabilities...” (8).

NATO forces routinely operate as expeditionary forces engaged in Allied joint operations, which occur both within and outside of the NATO area and responsibility. The operational environment may have no discernable “front lines” or “rear area” and an adversary may be expected to target Allied vulnerabilities anywhere with a wide range of capabilities. Security, one of the principles of operations, and protection, a key component of security, assumes an even higher importance in such environments. Force Protection (FP) is therefore defined as: “Measures and means to minimize the vulnerability of personnel, facilities, materiel, operations and activities from threats and hazards in order to preserve freedom of action and operational effectiveness thereby contributing to mission success.” (9). Thus, the fact is that NATO admitted that forces are vulnerable throughout the deployment, reception, staging, and onward movement, execution and redeployment phases of an operation – especially when infrastructure is not yet in place and information on the situation is incomplete (4).

So, if kinetic threats, which are physical in nature and are a type of threats that may require either proactive or reactive military actions, are eliminated on time we are no longer threaten and at least one of four forms of energy will remain an intact critical infrastructure. Additional neutralization of possible non-kinetic threats i.e. cyber-attack will accomplish the preventive actions and efforts in preserving strategic infrastructures circulating around four forms of energy.

Nevertheless, the Alliance and its forces remain vulnerable to a wide variety of hazards and threats. Hazards include occupational hazards such as road traffic accidents and fire and exposure to environmental hazards such as disease and Toxic Industrial Materials (TIM). A threat may be described as a state’s/coalition’s perception that is in some degree of danger based on the assessed capabilities, intentions, and actions of another state/coalition or group (9). Such threats may exist even in benign environments, such as unit’s home station or base. At best, an Improvised Explosive Device (IED) environment – or an environment that may involve Chemical, Biological, Radiological or Nuclear (CBRN) agents – may deter or delay the timely deployment of some national forces and undermine Alliance resolve. At worst, it may result in significant casualties and severely hamper or thwart mission accomplishment (9).

Survivability is therefore a principal consideration in strategic planning and decision-making – with implications that extend well beyond the military mission and into issues such as public support, political cohesion, and other areas. FP is based on risk management, not risk elimination. Casualties, deliberate or accidental, are a reality of military operations and the desire to avoid them totally may impact adversely the achievement of the mission. Although it is not possible to protect every asset against every threat all of the time, the assets previously identified as “critical to the mission” must be protected. As a part of FP, a comprehensive risk assessment process is essential to guide risk management decision-making prioritization (2, 3, 5).

From the scientific point of view and simultaneously using a pure common sense the serious question arises: “How vulnerable we are actually?” while NATO considered its vulnerability and pointed out such statement in its highly weighed strategic documents...

Adversaries may be expected to capitalise on perceived Allied weakness and vulnerabilities, giving rise to the need for a comprehensive and resilient strategy for the protection of forces. FP is essential to operations, and therefore a clear responsibility of command is to ensure that all military units are able to defend and to protect themselves appropriately against prevailing threats throughout the range of military operations. Hence, NATO’s operational needs and the increased global threat of terrorism prompted an urgent review (2, 3, 4).

It seems that national, regional and international interoperability and “know how” are no longer the adjective issue, is this true?

Restitution to solidly defined critical infrastructure: “Four forms of energy”, has grounded reason. We will try to offer some prudent reasons where the concept of “Four forms of energy” as an ultimate critical infrastructure has its weak points and hence the scenario can be diametrically different from the general expectation. We will enclose our further discussion about terrorism as number one phenomenon threatening the global security arena. Terrorism has already been scientifically described and defined to a certain level and any additional “invention” can diminish the major message we would like to launch to the wider audience (1, 6, 7, 10, 11).

In the light of nowadays threats (i.e. CBRN Devices) that differ rapidly and nearly on a daily basis, the term critical infrastructure calls for a detailed reconsideration. The critical infrastructures are more or less determined, representing mutual and essential principles for the command and control and the execution of multinational CBRN EOD operations. However, some professional remarks will be given regarding ambiguity of the current definition of the critical infrastructures in relation to natural or intentional outbreak of the highly contagious diseases.

Therefore, the major course of action declare: "It is about an ambition to use both, the infrastructure and human resources in order to achieve the highest level of security possible." (12,13).

### **Factors influencing strategic ambiguity of the term critical infrastructure**

Applying the term “know-how” into the “grey area” of mankind ratio and emotion has an infinitive possibility to become a complete absurd in the strategic definition of the critical infrastructure. Despite such serious possibility of scientific disqualification of the present paper we will remain in the “grey area” trying to provide some points of departure starting with “Goedel’s Theorem, which may belong to victims of a too one-sided approach to transforming novelties to innovations, so far.” Authors, Mulej et al (14, 15, 16, 17, 18) brief what system thinking and requisite holism actually is based on:

- Interdependences, Relations, Openness, Interconnectedness, Dialectical System;
- Complexity (& Complicatedness);
- Attractors;
- Emergence;
- Synergy, System, Synthesis;
- Whole, Holism, Big Picture, Holon;
- Networking, Interaction, Interplay.

The system approach is obviously supposed to enable people to think along the mentioned notions. Its point lies in prevention of oversights and resulting mistakes, including World Wars, and World Economic Crises, the climate change problem etc., but also a number of mistakes with less broad consequences (14). However, “law of requisite holism describes the natural fact, that human do not

have capacity to be totally holistic” (19). “On the other extreme, people hardly can do a good job, if they limit themselves to a single viewpoint, e.g. of a single profession with no co-operation with people who see the same processes differently. The right way, also in this case, is the middle way, but people must take responsibility for choosing a dialectical (i.e. interdependence-based) system of viewpoints of one kind rather than of another kind” (18).

What on earth have the alleged scientific facts of authors Mulej et al to do with the ambiguity of the term critical infrastructure? Almost everything!

The currently solid definition of critical infrastructure: “Four forms of energy” calls for re-consideration, especially when bio-agents (BA) dictate a style of thinking that has been unusual so far. Who will be the major target of potential biological warfare? The perfidious way of biological attack is simple but the reality of such kind of attack is far more complex than most humans are ready to face. It is not just about an intentional outbreak of the highly contagious disease. Humans are highly vulnerable to a non-hostile natural outbreak. World Health Organisation (WHO) finally admitted that antigenic shift of H5N1 had happened and the human-to-human transmission has engulfed the mankind (23). The “minority report” exceeded the doorstep where naive civilian population has been hypocritically misled that possible future pandemic is just an illusion, or worse, a delusional theory of some isolated scientists (20).

In meantime the Swine Plague has engulfed the Republic of Croatia in 2007. The major outbreak of the disease affected the geographic areas extremely close to the Slovenian national border. The “in real time” communication has failed and Slovenia was exposed to a threat fully close to a major disaster in which no single animal could survive/stayed alive: stamping out method is the only acceptable strategy in the case of such endemic. So, the national border with the Republic of Croatia became a critical infrastructure of a highest national priority. In addition, critical factors consist of each Slovenian veterinarian who crossed the border then (prior to Croatia’s official announcement of the outbreak of Swine Plague) and offered the vet-medical services to the each breeder; and vice versa (which is possible and a quite common illegal act close to the border), each single swine that has been in contact with any particular veterinarian in the Slovenian husbandry, any civilian person, any civilian close, any civilian footwear, any civilian vehicle that crossed the affected area, any transport in both ways, the entire nutrition chain, export and import et cetera.. Were we “lucky”? Fortunately no case of Swine Plague has been officially confirmed in Slovenia yet.

In addition, Slovenia faced (in 2007) the quite unexpected natural outbreak of Q-fever, a highly communicable disease, where animal-to-human transmission is a well-defined routine. This is just a foretaste of what Avian Influenza, Swine Plague, Q-Fever, Foot and Mouth Disease and other highly contagious diseases (bio agents) can and will demonstrate to the humanity of the 21<sup>st</sup> century. Soft - “Non Military targets” are nowadays target area of interest to dear fellow’s human beings. Therefore, the hypothetically doubtless but solid definition of critical infrastructure: “Four forms of energy” has another “side of the coin”. If some (intentionally anonymous) non-state actors provoke the intentional outbreak of the highly contagious disease to mankind, the “Four forms of energy” will remain perfectly intact. Covert release of BA with delayed effects will turn upside down each existing strategic document and the solid definition of “Four forms of energy” as a critical infrastructure: each course of actions will alter. The public will not notice this type of biological release until people start to become ill. A good awareness of such dangerous position among civilian population will end in panic, which cannot be perfectly predictable and in the vast majority of cases the arriving chaos will govern each security measures taken.

Civilians are those human resources who govern the solidly defined critical infrastructures: “Four forms of energy.” Destroying mankind with potential biological agent with delayed effects will protect the currently defined critical infrastructure that is vital to each adversary having its own reasons and strategic appetite to take it over. Mass casualties for what biological weapons are potentially made, are the main focus. No hostile track has the strategic concept, which will allow the end of “Four forms of energy”.

FP represents a safety zone in a certain level of course. The members of the Security/Armed Forces are well trained and equipped to protect themselves (4). However, they are only human beings. Their final task in the case of biological warfare might become a plain struggle to survive. And they can become ill as well; they can be part of the mass casualties as well. Empty space of the solidly defined

“Four forms of energy” can be the final outcome of the potential natural or intentional outbreak of the highly contagious disease of any inhabitant of the world.

That is why we dare to move the term critical infrastructure from nuclear plant, or as defined: “Four forms of energy” to human beings-animals-national borders-general transport etc. None of them exists and acts in isolation from each other; they are more inter-dependent than they look like at the first and shallow view. Their dialectical (i.e. interdependence-based) relations must stop being victims of oversights of specialists, who are deep inside their own specialties/viewpoints, but poor capable of interdisciplinary co-operation.

### **Holism of thinking, decision-making, and action**

Biological agents are an “invisible front” (21) seriously denying the currently recognized critical infrastructure. To be precise, we agree: “Four forms of energy” make a critical infrastructure. But this definition is somehow too decisive and one-sided rather than requisitely holistic. Another style of thinking was given just to remind or simply to add rather than to deny the highly strategic definition of critical infrastructure. Throughout history, infection diseases contracted naturally have had a significant impact on military operations and human lives. The effects of disease introduced to native populations were clearly demonstrated by the spread of smallpox in the Americas after arrival of Europeans and illustrated the potential impact of the deliberate use of BA (22).

The intentional dissemination of disease adds a new dimension to threats that are posed by BA traditionally transmitted only by natural routes. The global security arena is facing already the natural outbreak of virus H5N1, which crossed and it keeps crossing the national borders silently identically as electricity silently crosses the national borders giving the vital source of energy the absence of which can inflict a crisis of immense extension...

Proper planning often prevents poor performance, therefore, threat analysis, high readiness, tasking, coordination and prioritization remains the major factors when immediate strategic definition of a critical structure must be appointed. Proper, this means planning with requisite holism based on interdisciplinary creative co-operation. And: every planning, if it is proper, has to do with some innovation, at least, added to the established routine; the current life is no longer unchangeable like in old times.

“We just tried to demonstrate that holism of thinking, decision-making, and action is very necessary. Also, we would like to show how much more success one could yield in the innovation effort, if one applied more system thinking. The problem lies in mentality very much - in humans’ thinking and worldview as well as other values and other emotions.” (18).

“Take a look at experience around you and discover (again): Success has always resulted from absence of oversights with crucial impact. And failure has always resulted from crucial oversights, be it in business, scientific experiments, education, medical care, environmental care, invention-to-innovation processes, etc., or wars, all way to World Wars of 20<sup>th</sup> century, and all other wars and crises.” (18).

### **References**

1. Podbregar, I. (2005). Oblikovanje evropske strategije kolektivne varnosti. In: Lobnikar, B. (ed.). 6<sup>th</sup> Slovenian days of Security Studies. Bled, June, 2.-4. 2005. *Conference Proceedings*, pp. 1-6. Faculty of Criminal Justice and Security, Ljubljana, Slovenia. SI-ID 1060842]
2. Podbregar, I. (2003). Organisational aspect of common security in European Union. In: Florjančič, J. (ed.). 22<sup>th</sup> International Scientific Conference of Management and Organisational Development. Portorož, March, 26.-28. 2003. *Management and organisation development : collection of papers from international scientific conference on development of organizational sciences*, pp. 61-69. Moderna organizacija, Kranj, Slovenia. SI-ID 3823123]
3. Podbregar, I. (2000). Selection model for participants in peacekeeping operations. In: Jaškova, M. (ed.). *ECON '99 : Proceedings Book, selected research papers*, Vol. 6, No. 1, pp. 120-124. Technical University, Faculty of Economics, Ostrava, Slovakia. SI-ID 2751507]
4. Podbregar, I. (1999). Vojske prihodnosti. *Vojstvo*, No. 5, pp. 105-116. SI-ID 2518803]
5. Podbregar, I. (2000). Vloga oboroženih sil danes, jutri. *Defensor*, pp. 1-67. Defensor, Ljubljana, Slovenia. ISBN 961-6177-04-4.
6. Podbregar, I. (2004). Vloga obveščevalnih služb v boju proti mednarodnemu terorizmu. In: Lobnikar, B. (ed.). *Conference of Security Studies, Conference Proceedings*, pp. 30-34. Faculty of Criminal Justice and Security, Ljubljana, Slovenia. SI-ID 898794]

7. Podbregar, I. (2005). Metode delovanja obveščevalno-varnostnih sistemov v totalitarnem režimu : pregledni znanstveni prispevek na primeru SFRJ. *Slovenian Intelligence and Security Agency*, pp. 1-28. . Slovenian Intelligence and Security Agency, Ljubljana, Slovenia. ISBN 961-91646-0-1.
8. EDA CBRN EOD project Team. (2006). EU Chemical Biological Nuclear Explosives Ordnance Disposal Doctrine for Multinational Operation. EU, Brussels, Belgium.
9. NATO Standardization Agency. (2007). Allied Joint Doctrine for Force Protection: AJP-3.14. Third study draft. (2006). NSA, Brussels, Belgium.
10. Podbregar, I. Slapar, M. (2007). Razsežnosti gospodarskega vohunstva v 21. stoletju : primer gospodarskega vohunstva s pomočjo trojanskega konja. In: Lobnikar, B. (ed.) 8<sup>th</sup> Slovenian days of Security Studies. Bled, May, June, 30.-1. 2007. *Conference Proceedings*, pp. 1-6. Faculty of Criminal Justice and Security, Ljubljana, Slovenia. SI-ID 2750586]
11. Podbregar, I. (2006). Some patterns of industrial espionage. *Varstvoslovje*, Vol. 8, No.. 3/4, pp. 323-331. SI-ID 1324778]
12. Meško, G. (2004). Partnersko zagotavljanje varnosti v lokalni skupnosti- želje, ideali, ovire. *Rev Krim. Kriminol*, Vol. 55, No. 3. pp. 258-265.
13. Meško, G., Lobnikar, B. (2005). The contribution of local safety councils in crime prevention and provision of safety. *Policing*, Vol. 28, No. 2, pp. 353-373.
14. Mulej, M., Potočan, V., Ženko, Z. Ways to make the Goedel's theorem more known to people. (2006). University of Maribor, *Faculty of Economics and Business*. Maribor, Slovenia.
15. Mulej, M., Ženko, Z., knez-Riedl, J., Potočan, V. (2003). Upravljanje- kdaj je razmušljanje o njem in v njem sistemsko/celovito. *Organizacija*, Vol. 36, No. 7, pp. 443-445.
16. . Mulej, M., Potočan, V., Ženko, Z., Kajzer, S., Uršič, D., Knez-Riedl, J, Lynn, M., Ovsenik, J. (2004). How to restore Bertalanffian system thinking. (2004). *Kybernetes*, Vol. 1, No.33, pp. 48-61.
17. Potočan, V., Mulej, M. (2006). Enterprise competitiveness and ethics of sustainable development. In: Kickstarting small island enterprise competitiveness. The University of the West Indies at cave Hill. *Conference Proceedings*, pp. 299-314.
18. Mulej, M., Čančer, V., Hrast, A., Jurše, K., Kajzer, Š., Knez-Riedl, J., Mulej, N., Potočan, V., Rosi, B., Uršič, D., Ženko, Z. (2007). The law of requisite holism and ethics of interdependence: basic of the dialectical system thinking (applied to innovation in catching-up countries). (2007). University of Maribor, *Faculty of Economics and Business*, pp. 1-161. Maribor, Slovenia.
19. Mulej, M., Kajzer, S. (1998). Ethics of interdependence and the law of requisite holism. In: Rebernik, M., Mulej, M. (eds). *STIQE '98*. ISRUM et al. Maribor, Slovenia.
20. Podbregar, I., Ivanuša, T. (2007). The threat of pandemic is real if not inevitable – Who will protect the Security/Armed Forces in the case of Pandemic. In: TIEMS World Conference, Trogir. *Conference Proceedings*, p.p. 29-36.
21. Vauhnik., V. (1941). Nevidna fronta. *Knjižnica Novo mesto*. Novo mesto, Slovenia.
22. NATO Standardization Agency. (2005). NATO Handbook on the Medical Aspects of NBC Defensive Operations (Biological): AmedP6(C) Vol II. NSA, Brussels, Belgium.
23. WHO Confirms Human-To-Human Bird Flu Case Thursday a single case of human-to-human transmission of the H5N1 avian influenza virus in a family in Pakistan, but said there was no apparent risk of ... News, Reuters Health Information, December 2007.

### Authors:

OF-5 Military Specialist **Teodora Ivanuša**, Assist. Prof., DVM, M.Sc., Ph.D., Postgraduate Diploma of Criminal Justice and Security. Advisor for Education and Special Tasks, National Representative in NATO / CNAD / AC225 / JCGCBRN. Ministry of Defence, Slovenian Armed Forces; Doctrine, Development, Training and Education Command, Republic of Slovenia. teodora.ivanusa@siol.net.

Dr (systems theory in economics) Dr (innovation management) **Matjaž Mulej**, Professor Emeritus of Systems and Innovation Theory, University of Maribor, Faculty of Economics and Business, Maribor, Slovenia, member of 3 International Academies of Science and Arts, President of the International Federation for Systems Research (with 35 member associations and membership on all continents). Beyond 1.100 publications in beyond 40 countries. Visiting professor outside Slovenia for 15 terms. mulej@uni-mb.si