*Information & Security: An International Journal*

Iztok Prezelj, vol.33:1, 2015, 13-34 http://dx.doi.org/10.11610/isij.3301

# COMPREHENSIVE SECURITY AND SOME IMPLEMENTAL LIMITS

Iztok PREZELJ

**Abstract**: The changing security environment has led to the development of comprehensive security approaches, strategies and policies. The 'Holistic approach' has become an academic and practical mantra. This paper argues, however, that comprehensive security approaches face serious obstacles to their practical implementation. The critical evaluation of several examples confirms that the implementation phase is a weakness of comprehensive approaches and that a truly comprehensive and holistic approach seems to be beyond the implemental capacities of our security systems. Multi-sectoral and multi-level comprehensive approaches become less comprehensive when implemented in practice or even cannot be implemented due to existing narrow perceptions of security or narrow and short-term interests. The trans-sectoral second-, third- and fourth-order effects of proposed security measures are hardly considered or not considered at all. There is no consensus on what exactly comprehensive means, while prioritisation of some areas in the national security policy leads to de-prioritisation of other areas and new vulnerabilities, inter-organisational and cross-sectoral cooperation faces serious limits, threat, risk and vulnerability assessments are not really comprehensive, etc. This paper finishes with recommendations on what to do about these serious limits on the implementation of comprehensive security.

**Keywords**: Comprehensive security, multidimensional security, cross-sectoral approach, threat assessment, risk assessment, inter-organisational cooperation, critical infrastructure, asymmetric threats, counter-terrorism.

## Introduction

The end of the Cold War enabled the academic community and policymakers to redirect attention from typically military threats and problems to a much broader set of security issues. A comprehensive or holistic approach to security has since become a mantra in the field. Academic books, articles and studies have argued for a non-military and broader notion of security, while states and international organisations have created more comprehensive strategies and policies that lead to smarter and longer-term security. Progress in this direction has clearly been made, but we should also analyse this progress more critically to improve the academic understanding of existing weaknesses of comprehensive approaches. From this perspective, it seems that many smart comprehensive approaches have faced serious difficulties in the implementation phase. Arguably, a true comprehensive approach lies beyond humankind's implemental capacities at this stage of development.

I argue in this paper that comprehensive security approaches encounter serious obstacles to their implementation in practice. I should stress that I am a strong proponent of a comprehensive security approach (as confirmed by my research record), but my practical experience in the national security system with implementing broad and comprehensive security solutions led me to seriously consider implementation problems. The goal of this paper is to identify some typical difficulties of implementing comprehensive security approaches in practice and explain the reasons for them. Such work is relevant because it will create knowledge on the typical obstacles to implementing comprehensive security approaches and give ideas on how to overcome them.

## Comprehensive Approaches to Security

The neorealist focus on states and military security seems to fit the Cold War era perfectly, but the security environment has been changing continuously since then. Security concepts have reflected the changing threat perceptions. According to Williams and Moskos,[1] the key perceived threats were: a conventional military attack before the Cold War, a non-conventional military attack during the Cold War, and a broad spectrum of non-military threats after the Cold War (such as drug trafficking, uncontrolled migrations, economic stagnation, environmental degradation, etc.). The prevalent schools of security thought in the Cold War (realism and liberalism)[2] actually narrowed the problem of security to power (realism) and peace (liberalism), and security was thus mainly perceived as a politico-military problem. The nuclear threat was simply so great that such a confined understanding then seemed appropriate. After the 1980s, new security approaches (concepts and policies) gradually started to emerge. The old security concept proved to be too limited and unsuitable for the increasingly vibrant security environment. In this respect, the narrow security and strategic studies evolved towards much broader security studies, encompassing many non-military aspects of security. The prominent journals *International Security* and *Foreign Affairs* published two theoretically relevant articles both entitled "*Redefining Security*." Published in 1983 by Ullman, the first article substantiated the broadening of security to economic and developmental issues. He questioned the utility of focusing on military security since it conveyed a profoundly false image of reality and made states concentrate on military threats and ignore other and perhaps even more harmful dangers. He thought that such an approach actually reduces our overall security.[3] The second article was published in 1989 by Mathews, justifying a broadening towards environmental, resource and demographic issues.[4] Even the journal *Survival*, known for its neorealist approach, published an article in 1989 on non-military aspects of security. Perhaps the most comprehensive approach to security following the Cold War was substantiated by the "Copenhagen School" led by Barry Buzan, Ole Waever, Jaap de Wilde and others. In their key publications, such as "*People, States and Fear, An Agenda for International Security Studies in the Post-Cold War Era,*" "*The European Security Order Recast: Scenarios for the Post-Cold War Era,*" and "*Security: A New Framework for Analysis,*"[5] they defined security as an inherently multi-sectoral phenomenon consisting of:

- military sector (military threats and the means to contain them);
- environmental sector (e.g. environmental disasters);
- economic sector (e.g. economic recession, poverty);
- political sector (e.g. level of democracy); and
- societal sectors (e.g. cultural relations and identity).

The Copenhagen School was very important because it pragmatically combined traditional and emerging approaches in a new and more holistic approach to security studies. A positive aspect is that this school integrated the military dimension as it existed in the new broader context. Many other comprehensive approaches followed this multi-sectoral understanding of security.[6]

At the policy level, several broader security concepts were also introduced. The most notable examples were expressed in reports by the Palme Commission, Brandt Commission, and the United Nations Development Programme. The Palme Commission Report from 1982 represented a consensus of NATO, Warsaw Pact and neutral countries that no country can win in the case of a full-scale nuclear war. This report politically opened space for broader thinking on other potential security dimensions, such as economic security. In this respect, the Brandt Commission report from 1983 introduced economic security as a basis for achieving political security within countries and at the global level. More importantly, the UNDP developed and introduced the "people-centred" "all-encompassing concept of human security" in its annual report from 1994.[7] UNDP employed bottom-up logic and tied the concept of security to the individual and his day-to-day life, including the most pressing daily threats. The concept referred to these dimensions of security: economic, food, health, environmental, personal, community and political. A comparison of human security concepts [8] regarding the perceived and identified threats to individuals shows a great variety of potential threats. All approaches stress mostly non-traditional threats; yet traditional ones are also mentioned and stressed by some. The threat spectrum encompasses the following threats: economic, food, health, environmental, personal, community, political, demographic, as well as crime in all forms, including terrorism, natural disasters, violent conflicts and wars, genocide, anti-personnel mines, SALW, etc. The human security concept refocused attention in security studies on the vulnerability of individuals rather than on governments and territories. Individuals are the most vulnerable referent objects of security.[9] UNDP also equated human development, peace and well-being. This all reflects the fact that broader security concepts were grounded in the intellectual drive of the Cold War era aimed at shifting the focus of national security from the state-centred approach to security for society, communities and individuals.

After 9/11, the concept of asymmetric threats also became increasingly recognised and used by the scientific community worldwide. This concept appeared in the USA in the late 1990s. It was quickly exported to other countries and represents one of the key ways of understanding threats in the 21st century. Asymmetry here refers to the disproportionality between the threatening subject and the threatened subject, which mainly refers to terrorists on the offensive side, and the state and society on the defensive side.

What actually happened with security at the conceptual and policy level after the Cold War ended is a simultaneous horizontal and vertical broadening of the term. Horizontal broadening refers to incorporating 'new' non-military aspects of security such as environmental, economic, demographic, criminal, terrorist, health, information, immigration and other aspects (or sectors and dimensions as some call them), while vertical broadening refers to the incorporation of other non-state referent objects like individuals, local communities, groups of people by common ethnic, religious or ideological characteristics, the global community, etc. This combination of non-military security dimensions and non-state referent objects represents the basis of today's comprehensive understanding of security.

The EU and its member states have also adopted a comprehensive approach to security. WEU security functions were transferred to the EU at the start of this millennium, and the EU further developed its civil and military crisis management functions, including counter-terrorism, critical infrastructure protection, etc. Two very important documents should be mentioned here because they underpin the EU's comprehensive approach to the field of security. The European Security Strategy set the foundations for the comprehensive approach to external security by identifying a comprehensive spectrum of security threats (terrorism, proliferation of WMD, regional conflicts, state failure, organised crime, etc.) and stressing a more coherent approach and coordination among various EU policies (especially external action and Justice and Home Affairs policies), the external activities of individual member states and also regionally.[10] The Internal Security Strategy later comprehensively defined the common internal security strategy and the model of European security. The document called for integrating existing strategies and exploiting potential synergies that exist in the inseparable areas of law-enforcement cooperation, integrated border management, and criminal justice systems. The purpose of this document was to ensure that these areas complement and reinforce one another.[11] The EU has also pursued a comprehensive approach in other policies, such as "comprehensive and geographically balanced EU external migration policy"[12] or the comprehensive implementation of peace agreements.[13] At the level of EU member states, numerous examples of a comprehensive approach to security can be identified. For instance, countries follow a model of comprehensive and interconnected use of the whole spectrum of political, military and civil mechanisms for managing the interconnected problems of peace, security, development and human rights. Interagency cooperative processes among ministries of foreign, defence and internal affairs have been established.[14]

In the case of complex security issues, a concern has been raised about who actually 'owns' them. The answer is everybody and nobody. 'Everybody' refers to all relevant stakeholders, governmental, non-governmental and supra-governmental, while 'nobody' refers to the fact that none of them can claim complete ownership of the problem due to their own, individual inability to solve it. From this perspective, in the future comprehensive security policy decision-making will be challenged by many problems and face significant uncertainties. According to Kugler, best policies will be formulated when competing views or camps can be synthesised by combining them in a sensible whole. However, he also stressed that the adopted policy options need to be implemented, which sometimes turns into a lengthy and complicated problem.[15] The application of different decision-making models to the security field has shown the existence of many reasons why decision-making in complex situations can fail. To take a few examples,[16] the cybernetic theory has shown that decision-makers have limited capabilities for rational decision-making. The prospect theory demonstrates that decision-makers will think not only about solving the problems, but also about their personal and political gains and losses. The groupthink model has stressed the importance of loyalty to real or perceived group norms that could take over the rational decision-making. The bureaucratic politics model has suggested that the decision-making process is also a consequence of competition among the actors.

The term "whole-of-government" approach has also been used to reflect the need for comprehensive decision-making far beyond the sectoral and governmental interagency approach. In the field of emergency preparedness, Perry and Lindell defined "community emergency preparedness" as a comprehensive process in which all relevant organisations need to be involved as part of effective inter-organisational coordination.[17] Comprehensive decision-making in the internal security field, as defined by the EU Internal Security Strategy, contains a horizontal and a vertical dimension. The former involves law-enforcement and border-management authorities, with the support of judicial cooperation, civil protection agencies and also of political, economic, financial, social and private sectors, including non-governmental organisations. In contrast, the vertical dimension includes international cooperation, EU-level security policies and initiatives, along with regional cooperation between member states' own national, regional and local policies.[18] In the case of complex security questions related to critical infrastructure, the approach based on Public-Private Partnerships (PPP) has been extensively used in practice. Without such a wide approach, critical infrastructures cannot be secured against a broad range of contemporary threats.

## Some Difficulties of Implementing Comprehensive Security Approaches

In this section, certain key topics have been selected to show the limits of comprehensive security approaches in practice. Some practical limits are a direct consequence of the theoretical challenges.

### *Multidimensional Security is Not New and is More Complex than Expected*

We should remember the "new threats to security" rhetoric used by many scientists and professionals after the Cold War ended. They claimed that after the end of the Cold War there are actually new threats to security such as crime, environmental threats, economic threats, immigration threats etc. Many policy strategies and documents reiterated this view. For example, the European Security Strategy stressed that Europe faces "new" security threats which are more diverse, less visible and less predictable than the threat of a large-scale aggression.[19] However, most of the mentioned threats and security dimensions already existed during the Cold War. They were just not prioritised in the academic literature or in the security discourse. This brings us to the constructivist view that security is what we think or say it is, and that our understanding of security is actually a social construction. The problem is that it was not understood that it is more about the reprioritisation of security policy than a change in reality. There was only one sector which was truly new in terms of security and non-existent during the Cold War: the information sector with cyber threats to security. This means that the birth of comprehensive multi-sectoral security was accompanied by a false perception of novelty, while in reality only our focus has changed. The practical consequence of this has been great fascination and expectation about the benefits of securitising the environment, the economy, immigration, health etc. In reality, these fields have only been partially securitised. National security policies include them in the security framework, but mostly as secondary sectors compared to more traditional ones. Broader security frameworks automatically triggered the problem of inter-sectoral competition, which will be addressed later.

At this point, we can offer an example of the prioritisation with serious consequences. One state with the most developed security in the world, the USA, prioritised the terrorism issue after 9/11 and deprioritised emergency management in the case of disasters. Hurricane Katrina would not have had such drastic consequences in New Orleans if the levees had been properly maintained. Today, we know that a multi-sectoral approach to security is the right approach, but in practice we do not sufficiently understand the second-, third- and fourth-order links among security sectors. For example, do we in 2015 understand how the use of the military to protect EU borders from immigrants in order to reduce the inflow will also affect crime in the countries of origin and in the target countries, how it will affect the ongoing conflicts in the countries of origin, how it will affect the level of democracy and human rights, whether by closing our borders we can actually increase the probability of democratic changes or prospects for revolution or new conflicts. These are all trans-sectoral complex questions that are mostly not dealt with when addressing specific problems. The second example is Afghanistan. How is it that NATO countries have been unable to eradicate the poppy fields in Afghanistan (this would be part of military action) while at the same time our national police services and EUROPOL have assessed that the main inflow of heroin still comes from Afghanistan. Well, if NATO forces were to do this then the main Afghani economic branch (agriculture) would collapse and the entire stabilisation and peacebuilding process would be endangered. In this case, the political inconveniencies of a truly broad approach to security have in fact prevented the broad approach being implemented. And the third example of the inability to understand the multidimensional approach comes from the counter-terrorism field. The policies of targeted killings of terrorist and extremist leaders applied by some states (e.g. the USA and Israel) turned out to only be effective in the short term and only when viewed from the narrow perspective. This approach has effectively eliminated some very important terrorist leaders, but the problem of the terrorist threat will still remain because they are unable to win the hearts and minds of the population nor do they know how to integrate a human security approach into their national security and counter-terrorism policy. In fact, the big collateral damage from such policies has increased the motivation for terrorism against such states and their apparent allies, thus indicating a failure to understand the complexities of contemporary terrorism. Security reactive measures have obviously not been adequately connected to long-term preventive measures.[20] Another bit of proof on this point: the most ‘successful’ countries in counter-terrorism (with known successful operations, well-trained special forces, etc.) have always been the most threatened countries.

### How Comprehensive is ‘Comprehensive’ Remains Unclear

One would expect some kind of consensus in the security literature on what a comprehensive approach means, what it includes, etc. The broad approaches to security elaborated above are not entirely comprehensive and occasionally overlook some dimensions or sectors mentioned by other authors. For example, the Copenhagen

School, promoting probably the most comprehensive academic approach to security in the post-Cold War era, has completely neglected the cyber dimension. Its proponents have also deprioritised the dimension of crime and terrorism. The main problem is that ‘comprehensive’ includes all aspects of security, but nobody actually has the power to implement all aspects of security. Authors have warned that we would face the inflation of the concept of security were we to include all disintegrative events in the security framework[21] and that concept’s coherence would then be threatened. Walt defined several risks and challenges of broadening the term ‘security’ after the end of the Cold War and warned that security studies need to reflect on the ongoing changes.[22] Prins, Terriff and colleagues categorically concluded that security studies have changed from being a sub-discipline of International Relations to a fragmented approach with many different perspectives that are not necessarily in constructive dialogue (e.g. realism, liberalism, feminism, peace studies, strategic studies, etc.). These theoretical approaches talk past each other despite them having the same focus – security.[23] These and similar conclusions have led some authors to stress that a reduction of the concept of security is necessary in practice[24] and that an environment of endless threats and limited security means that some security aspects need to be extracted and further focused on.[25] Something similar has been found for the greatly promising human security concept. This concept also includes almost all aspects of security at the conceptual level, which has led to the problem of focus and implementation in practice. While the human security concept is theoretically well substantiated, attractive and modern, it embraces almost everything, making it difficult to put it into practice.[26] The practical consequence of this is the conscious or unconscious move from theoretically and logically comprehensive approaches to comprehensive approaches implementable in practice.

One very dramatic example can be given here. The concept of the Revolution in Military Affairs was developed in the 1990s to steer a comprehensive military reform process. The concept encompassed all aspects of military change: organisational, operational, financial, technical and doctrinal. A comparative study of 33 countries in the period 1992–2010 showed that in practice there was no comprehensive revolution in military affairs. In fact, in practice contemporary armed forces predominantly faced an incremental evolution with very rare major (revolutionary) shifts.[27]

### Asymmetric Threats Are Not New; Prioritising Asymmetric Threats Is Risky

As mentioned, the concept of asymmetric threats has become increasingly recognised and used by the scientific community worldwide and most modern states in their national security policies. Contemporary states now supposedly face very smart and dangerous threats in the form of terrorist groups and cells, ethnic groups, individuals, etc., who use innovative means to attack the weaknesses and undermine the strengths of stronger opponents. Asymmetry refers to the disproportionality in capacities and size between the threatening subject and the threatened subject.[28] In my view, the problem with overemphasising the asymmetric character of contemporary threats comes from a lack of awareness of the history of security threats. From the historically holistic perspective, we can see that asymmetric threats have existed for a very long time in human history. Even Sun Tzu, in one of the oldest existing sources on strategy, argued for asymmetric approaches. For example, he advised finding the opponent's vulnerable spots where victory will be easily achieved, to attack only what is vincible and where no defence exists, to attack when the opponent is not expecting an attack, he also argued that winning without a fight and only with a strategy is best, etc.[29] This means that asymmetric threats are not new in the contemporary security environment.

If countries focus their national security on particular asymmetric threats (e.g. terrorism) they will simultaneously deprioritise other threats (e.g. when the USA deprioritised disaster management after 9/11 and Hurricane Katrina created unimaginable damage). The current prioritisation of non-military threats in national security policies may seem logical because there has been no clear and present military threat to European countries. But if we look at the situation from the historically holistic perspective, we can assume that this policy makes Europe militarily vulnerable and brings new risks. The military threat by other states will in one way or another be present in our security environment and we should not forget this. Let me give a current example. The potential outbreak of a major international war in Ukraine with NATO countries on one side and Russia on the other finds several NATO countries quite unprepared. One may question how well the forces of some NATO countries would be able to fight other military forces in a military conflict and what level of public support they would have.

### *The Limits of Interdisciplinary and Inter-organisational Cooperation*

The lesson arising from the terrorist attack on the World Trade Center (WTC) and the Pentagon in 2001 concerns the need for greater inter-organisational cooperation in providing security. The global security environment is perceived as complex due to the many potential threats. Comprehensive solutions have been defined as multidisciplinary at the conceptual level and multi-organisational at the practical level. Yet, the 'multi' approaches are insufficient; academic disciplines need the ability to interact interdisciplinary and security organisations (governmental, international organisations and NGOs) – inter-organisationally. Such horizontal cooperation has become a mantra in security studies, but the practical problem of implementation emerges again. It seems that the national security policies of modern states are generally able to only implement moderate interdisciplinary and inter-organisational approaches. Let us consider the case of counter-terrorism.

The terrorist attack on the WTC and the Pentagon in 2001 was made possible by the low inter-organisational cooperation within the US national security system. The 9/11 Commission Report called for "greater unity of effort" in sharing information.[30] The Bush Administration established various interagency bodies (the Terrorist Threat Integration Center, The National Counterterrorism Center, The Homeland Security Council, The National Intelligence Director, intelligence fusion centres, etc.) to improve horizontal cooperation among the decentralised agencies.[31] Other governments and ministries around the world have expanded their horizontal communications and established coordination bodies.

The EU also identified the same lesson due to terrorist attacks on its own ground, and carried out an EU-wide peer evaluation of national counter-terrorist arrangements that resulted in recommendations to all member states to enhance the interagency exchange of information at the national level, increase the interagency transparency of various governmental databases, and set up a national coordination body responsible for the daily exchange of information.[32] A subsequent comparative analysis of national counter-terrorism practices showed that by 2005 14 out of 27 EU countries had already instituted their respective inter-agency counter-terrorism body, whereas only two had existed before 9/11.[33] An additional stimulus for improving counter-terrorist activities at the EU level came from the lessons of the attacks in London in 2005. In the aftermath of this attack, the EU adopted its counter-terrorism strategy, which comprehensively defines the EU's counter-terrorism activities in four strands or pillars: prevention, protection, pursuing and response. The Strategy also requires some kind of proportionate comprehensiveness, expressed by the following strategic commitment: "*To combat terrorism globally while respecting human rights, and make Europe safer, allowing its citizens to live in an area of freedom, security and justice*."[34] The Strategy requires work at national, European and international levels to reduce the threat from terrorism and vulnerability to attack. In 2015, EU counter-terrorism is based on close coordination between internal and external action on one hand and between relevant EU actors and EU member states on the other.[35] Internal counter-terrorism has been increasingly integrated primarily with the external security dimension.

Moreover, many professionals and academics started repeating the mantra of horizontal inter-organisational cooperation and coordination in the fight against terrorism. For example, it was stressed that the "counterterrorism organizational landscape"[36] should embrace a "full range of means"[37] such as intelligence services,[38] law enforcement,[39] diplomacy,[40] military,[41] emergency services,[42] and the related coordination bodies. It was recognised that the terrorist threat cuts across the political, legal and institutional jurisdictions of these actors and that the old vertical approach could no longer work without being reconceptualised. There were also calls to create new response networks,[43] partnerships among the traditional bodies of national security,[44] and a truly integrated and multifaceted approach that combines all counter-terrorism activities.[45] Hoffmann also argued that a critical step in efficiently addressing contemporary terrorism would come from a multi-dimensional policy and strategy able to build bridges within one's own governmental structure, untangle lines of authority, de-conflict overlapping responsibilities, and synchronise inter-agency operations. He proposed the creation of a counter-terrorism strategy based on the integration of a military kinetic force and the non-kinetic contribution of national power.[46]

Several general and also practical assessments of the achieved level of inter-organisational cooperation in counter-terrorism reflected serious limitations of the comprehensive approach. For example, it was found that organisational confusion remains a perennial problem in counter-terrorism networks,[47] that these networks are still not fully understood entrepreneurial or experimental entities in comparison to the prevalent hierarchical organisations,[48] and that the integration of counter-terrorism tools is still in an extremely primitive phase despite the investment of great efforts in horizontal, inter-organisational and network counter-terrorism.[49] Kramer even metaphorically labelled counter-terrorism networks as the tragedy of information communities, due to their inherent inability to resolve related coordination and cooperation problems.[50] In 2007, the EU Counter-Terrorism Coordinator reported on the persisting and insurmountable cooperation and coordination problems in Europe's national counter-terrorism communities, and many authors reported similar difficulties from the USA. It was also made clear that the complex organisational structure of the EU continues to hinder the coordination of international counter-terrorism activities within the EU. The mechanisms of cross-pillar or cross-dimensional cooperation have been created, but their coordination has not been optimal. This problem has to some extent also been a consequence of insufficient interministerial or interagency cooperation in the member states.[51]

A SWOT assessment of the effectiveness of inter-organisational cooperation in counter-terrorism after 9/11, based on the opinion of 100 counter-terrorism experts from many states, showed that there has been significant progress in this field, but at the same time inter-organisational cooperation suffers from serious weaknesses. Sharing information in the counter-terrorism community and mutual trust were identified as simultaneous strengths and weaknesses. This suggests that the counter-terrorism community is effective and ineffective with regard to the same points: information is exchanged, but not sufficiently, organisations trust each other, but not really. This indicates that the 'uncooperative' symptoms that led to 9/11 continue to remain hidden under the surface of cooperation, and that a new 9/11 could happen again. It also means that the terrorist threat itself has united the responsible actors, but only to some extent. From this perspective, truly effective inter-organisational cooperation seems like the holy grail of modern counter-terrorism: ever sought, but never really found.[52]

## The Limits of a Comprehensive Approach to Critical Infrastructure Protection

The contemporary holistic understanding of security also entails critical infrastructures which consist of basic socio-technical systems, organisations and networks that vitally support a large spectrum of human activities. They include transport (road, rail, air, sea) infrastructures, telecommunication systems, information systems (e.g. the Internet), energy (electricity, gas, oil) systems, financial and bank systems, food supply chains, water supply systems etc. These infrastructures are so vital that their breakdown or partial or complete failure would pose a serious threat to society and a major crisis at the national and even international level. This is why all modern states have developed a critical infrastructure protection policy to prevent and respond to accidents, attacks and failures that could take place in any sector of critical infrastructure.[53] Further, the European Commission has developed a policy for the protection of European Critical Infrastructures.[54] Typical threats considered in relation to critical infrastructures are intentional attacks (e.g. terrorism, information attacks, crime etc.), serious technical faults or malfunctions in systems, and accidents or disasters.[55]

The problem concerning a comprehensive approach in this field arises from the infrastructural complexity and unpredictable cross-sectoral interaction of infrastructural malfunctions. On several occasions, it was suggested to shape a comprehensive critical infrastructure protection policy and cross-sectoral approach based on an integral and interconnected preparedness,[56] a network approach,[57] a “system of systems” approach[58] and an integral approach based on cross-sectoral similarities.[59] However, considerable policy fragmentation has been observed in this field due to the large institutional fragmentation and lack of multidisciplinary integrated analysis at the national and international levels.[60] Countries have established governmental interagency bodies for critical infrastructure protection, but the regulation and management of all these infrastructures remains in the hands of ministries or even private actors. This explains why cross-sectoral similarities have not been taken into consideration to a large extent when implementing integral policy.

Many studies on infrastructural interdependencies have been commissioned by European governments and the EU and our understanding of cross-sectoral effects after infrastructural malfunctions has been improved, but the implementation of interdependency-based critical infrastructure protection policy still suffers from the lack of interdependency elements, such as identification of multi-critical infrastructural objects and links, cross-sectoral intersections, the cross-border cross-sectoral transfer of malfunctions, etc. The latter means that international critical infrastructure protection policy should also focus on intersectoral cross-border cooperation (e.g. between managers of ICT from one state and of electricity from another), and not just on international cooperation within the same subsector.

The European Commission's attempt to create a comprehensive European approach was also blocked by the member states due to their national interests. The Commission initially proposed the identification of European critical infrastructures in many infrastructural sectors, as shown in Table 1 below.

It was not possible to ratify the Directive with all these sectors and sub-sectors due to a number reservations expressed by some European states. In the discussion on the criteria for determining European critical infrastructure (in which the author's research group also participated), it was obvious that, in comparison with smaller states, some bigger states were not interested in having many critical assets. They assumed this would mean additional costs and problems. Consequently, the determined thresholds were very high and the directive that was adopted on European critical infrastructure from 2008 only included the sectors of transport and energy (with the promise that ICT would be included in the future). This is how the comprehensive multi-sectoral approach to protect European critical infrastructure failed.

## *Limits of Comprehensive Threat, Risk and Vulnerability Assessment Tools*

In all security fields, academics and stakeholders assess and discuss threats, risks and vulnerabilities. For example, what threat does Iran with nuclear weapons represent to the West, what are the risks of letting Iran retain its military nuclear programme and which vulnerabilities of the West could be targeted by a nuclear Iran. Understanding threats, risks and vulnerabilities is the cornerstone of a comprehensive security assessment and the basis for smart decision-making at national or international level (e.g. by international organisations). Assessment of these categories has been frequently carried out in a very simple way and without any methodological considerations. On the other hand, some stakeholders use very sophisticated methodologies to form a comprehensive understanding of what is going on. From this perspective, threat assessment typically includes evaluating the malicious intentions or motivations of actors and their capabilities to carry through on them. Threat assessment can be applied in all of the security dimensions or sectors mentioned above (provided we have a human-based threat). Risk assessment typically refers to the likelihood that a threat will escalate and create impacts. Vulnerability assessment focuses on susceptibilities to injury or attack, flaws or weakness in system security procedures, design, implementation or internal controls that could be accidentally triggered or intentionally exploited. Vulnerability is from this perspective a characteristic of the threatened object (state, system etc.) that renders it susceptible to destruction or incapacitation by a threat.[61]

Table 1: Proposed sectors and sub-sectors of European critical infrastructure as part of a potential comprehensive European approach.[62]

| *Sector* | | *Product or service* |
|---|---|---|
| I | Energy | 1 Oil and gas production, refining, treatment and storage including pipelines |
| | | 2 Electricity generation |
| | | 3 Transmission of electricity, gas and oil |
| | | 4 Distribution of electricity, gas and oil |
| II | Information, Communication Technologies, ICT | 5 Information system and network protection |
| | | 6 Instrumentation automation and control systems (SCADA etc.) |
| | | 7 Internet |
| | | 8 Provision of fixed telecommunications |
| | | 9 Provision of mobile telecommunications |
| | | 10 Radio communication and navigation |
| | | 11 Satellite communication |
| | | 12 Broadcasting |
| III | Water | 13 Provision of drinking water |
| | | 14 Control of water quality |
| | | 15 Stemming and control of water quantity |
| IV | Food | 16 Provision of food and safeguarding food safety and security |
| V | Health | 17 Medical and hospital care |
| | | 18 Medicines, serums, vaccines and pharmaceuticals |
| | | 19 Bio-laboratories and bio-agents |
| VI | Financial | 20 Payment services/payment structures (private) |
| | | 21 Government financial assignment |
| VII | Public & Legal Order and Safety | 22 Maintaining public & legal order, safety and security |
| | | 23 Administration of justice and detention |
| VIII | Civil administration | 24 Government functions |
| | | 25 Armed forces |
| | | 26 Civil administration services |
| | | 27 Emergency services |
| | | 28 Postal and courier services |
| IX | Transport | 29 Road transport |
| | | 30 Rail transport |
| | | 31 Air traffic |
| | | 32 Inland waterways transport |
| | | 33 Ocean and short-sea shipping |
| X | Chemical and nuclear industry | 34 Production and storage/processing of chemical and nuclear substances |
| | | 35 Pipelines of dangerous goods (chemical substances) |
| XI | Space and Research | 36 Space |
| | | 37 Research |

The problem with the above assessments is that there is no unified methodology for a threat, risk and vulnerability assessment. For example, while there is an EU comprehensive risk assessment procedure (actually, an ISO standard) applied in all member states in the field of civil protection,[63] it only represents one of the methodologies used in practice. The difficulty is that a broad spectrum of applied assessment methods leads to a broad spectrum of not necessarily similar results. Any such comprehensive threat, risk or vulnerability assessments will therefore suffer from the non-comprehensive character of the method used. Consequently, the validity of any comprehensive security assessment can be easily disputed simply by using another equally appropriate method that leads to somewhat different results.

Another question is the maturity of our national security systems to implement comprehensive threat, risk and vulnerability assessments. Here we can mention an example from Slovenia, where a research project on comprehensive threat assessment in 2006–2007. It was in Slovenia's interest to develop a procedure or system for comprehensive, permanent and complex threat assessment in several security dimensions (a multidimensional approach). The author of this paper led a multidisciplinary research group with security experts from different dimensions (military, crime, terrorism, natural disasters, economy, immigration, health) supported by mathematicians and information specialists. This group identified threat indicators in cooperation with 30 institutions from the broader Slovenian national security system. A prototype of the computer program INTEGRO was written and presented to the national security community. The program was based on the following functions:

- inserting several hundred threat indicators by operatives from different national security institutions (multidimensional input) at any time and based on individual passwords;
- analysing individual indicators in time and more complex correlational and interdimensional assessments (e.g. does the number of foreign fighters in the terrorist dimension correlate with economic indicators or immigration indicators); and
- displaying these indicators in various graphical forms to the country's top leaders.

The validity of this comprehensive threat assessment approach stemmed from the SMART indicators (Specific, Measurable, Agreed, Realistic and Timely). The purpose of having such a complex and comprehensive threat assessment system was to enable the most senior state leadership to monitor the security situation in real time by simply clicking on indicators in all relevant security dimensions.[64] This sounds like almost a perfect solution for a complex need, but neither at the right time nor the right place. Since the project ended, the high officials from the national security system and key politicians have not recognised the usability of such a tool. For some individuals coming from various subsystems and having adopted a narrow and interest-based understanding of security (in which protecting their turf is one of the most important things) such an out-of-the-box solution seems like unnecessary and even unfriendly theoretical idea. One of them said at the presentation meeting that the INTEGRO program created uncomfortable feelings that his institution would give some sensitive security information away to the government. In his view, this could be even illegal (if personal information were included in the threat indicators, but this was not the case). The implementation of this idea for a comprehensive threat assessment in the national security system of Slovenia—EU and NATO member state—was halted due to sectoral views of security, narrow institutional interests and perhaps also due to an incapacity to understand security in truly broad terms.

Here another question emerges as to whether our societies and governments really want to have and see comprehensive threat, risk and vulnerability assessments. What if an uncomfortable number of threats is to some extent paradoxically created by our national (security) policies. In such a case, threats strike like a cross-sectoral boomerang. For example, a state had a colony in the past, created the basis of the colonial domestic political system with all its present deficiencies, exploited the country and carried out some crimes and now it faces an uncontrollable flow of illegal immigrants from that country. Or, an example of a country which has assertive national interests all over the world creates injustices there (actual or perceived) and then faces a terrorist response and becomes one of the most threatened countries in the world. An interest-based view of security can never entirely be a comprehensive view of security.

## Conclusion and Some Ideas for How to Overcome the Limits to Comprehensive Security

This paper tested the argument that comprehensive security approaches face serious implementation obstacles in practice. This argument can be confirmed based on the analysed examples. The critical evaluation of several comprehensive approaches and concepts shows that a true comprehensive and holistic approach in practice lies beyond the implemental capacities of our security systems. This means that multi-sectoral and multi-level comprehensive approaches become somewhat less comprehensive when implemented in practice or even cannot be implemented due to existing narrow perceptions of security. The paper has shown that comprehensive approaches can sometimes be too complex to implement. The trans-sectoral second-, third- and fourth-order effects of proposed security measures are hardly considered or even not considered at all. There is no consensus on what exactly comprehensive means and how comprehensive is ‘comprehensive.’

A broad approach to security has resulted in a wide array of approaches talking past each other and also leads to the lack of focus. The so-called ‘new approaches’ (new threats to security, asymmetric threats) are actually not new. They are predominantly a result of changed perceptions and not so much of a changed reality. Prioritisation in national security policy seems a logical approach to meet the security challenges, but it simultaneously means deprioritisation of some other approaches that are still relevant in the long term. While prioritisation brings efficiency, deprioritisation brings new vulnerabilities that will re-emerge and challenge our security systems in a few years. The so strongly advocated solution to complex threats in the form of inter-organisational and cross-sectoral cooperation (including by the author of this paper) has led to improvements, but the effects of this idea have been simultaneously limited by our mental, legal and bureaucratic concepts. Although we teach specialised sectoral thinking in schools at all levels, our security officials are mostly trained in a sectoral manner (to achieve sectoral goals), they defend their turf and sometimes compete with other sectors for prestige, power and budgets. All of these factors limit the success of the mantra of inter-organisational cooperation.

Critical infrastructure protection policy and related integral network approaches suffer from organisational and technical complexity. Progress towards a truly comprehensive approach will be slow in this field. And last but not least, a comprehensive threat, risk and vulnerability assessment seems like a good theoretical idea. In practice, many assessment methods exist and lead to somewhat different assessments, they sometimes even compete and undermine each other’s comprehensive character. The question is also whether our societies and policymakers really want to have realistic and comprehensive threat, risk and vulnerability assessments on the table. In the case of threats, risks and vulnerabilities directly created by following own national interests, such holistic assessments would be a disturbing factor limiting the effectiveness of the pursuit of these interests. Several examples in this paper have shown that an interest-based view of security cannot entirely make up a comprehensive view of security. In other words, it seems that all comprehensive policy approaches cannot be comprehensive because they likely do not serve a comprehensive policy interest. From this perspective, a truly comprehensive approach in security studies seems like the holy grail: ever sought, but never really found.

This paper used only a few examples to improve our awareness of the limits of comprehensive security approaches. Several others could be included, such as the limited national capacities to create comprehensive national crisis management systems, limited practical ability of the European national security systems to strike a balance between security and human rights or to provide maximum security with minimal or zero violations of human rights. The limited value of comprehensive planning for complex crises and emergencies could also be highlighted. However, adding such cases would have considerably extended the paper's length.

The final question is: what shall we do about the realistic conclusion on the serious limits to implementing comprehensive security? The reality is that there is no alternative to comprehensive security approaches. We need to improve these concepts and try to implement them. A smart comprehensive security approach seems to be one that also includes a comprehensive implementation plan. In the implementation phase, we need to monitor the progress critically and reflect all the problems. Such reflections need to explain the reasons for failures and difficulties. We need to educate students and policymakers on the need for a comprehensive approach, the negative consequences of sectoral approaches to complex issues, on the value and pitfalls of inter-organisational cooperation, as well as the positive and negative effects of prioritisation in security policies. In addition, considerable attention should be devoted to developing methodologies for identifying and assessing the cross-sectoral second-, third- and fourth-order effects of potential security measures. In this way, smarter and longer-term security can be achieved in the future.

## Notes

[1] John Allen Williams and Charles Moskos, "Civil-Military Relations after the Cold War," in *Civil-Military Relations in Post-Communist States: Central and Eastern Europe in Transition*, ed. Anton Bebler (London: Praeger, 1997).

[2] Terry Terriff, Stuart Croft, Lucy James and Partick Morgan, *Security Studies Today* (Cambridge: Polity Press, 1999).

[3] Richard Ullman, "Redefining Security," *International Security* 8, no. 1 (1983): 129-53.

[4] Jessica Mathews Tuchman, "Redefining Security," *Foreign Affairs* 68 (1989): 162-77.

[5] Barry Buzan, Ole Waever and Jaap de Wilde, *Security: A New Framework for Analysis* (London: Lynne Rienner Publishers, 1998); Barry Buzan, *People, States and Fear, An Agenda for International Security Studies in the Post-Cold War Era* (London: Harvester Wheatsheaf, 1991); Barry Buzan, Morten Kelstrup, Pierre Lemaitre, Elizabeta Tromer and Ole, Waever, *The European Security Order Recast: Scenarios for the Post-Cold War Era* (London: Pinter Publishers, 1990). Also see Hakan Wiberg, "Security Problems of Small Nations," in *Small States and the Security in the New Europe*, ed. Werner Bauwens, Armand Clesse and Olav Knudsen (London: Brassey's, 1996).

[6] For a good elaboration on security schools, see Steve Smith, "The Increasing Insecurity of Security Studies: Conceptualizing Security in the Last Twenty Years," in *Critical Reflections on Security and Change*, ed. Stuart Croft and Terry Terrif (London: Frank Cass, London, 2000).

[7] UNDP, *Human Development Report* (New York: Oxford University Press, 1994), 24.

[8] Iztok Prezelj, "Challenges in Conceptualizing and Providing Human Security," *HUMSEC Journal* 1, no. 2 (2008), accessed on 3 December 2010, available at www.humsec.eu/cms/fileadmin/user_upload/humsec/Journal/Prezelj.pdf.

[9] Astri Suhrke, "Human Security and the Interests of States," *Security Dialogue* 30, no. 3 (1999), 265-76.

[10] Council of the EU, *European Security Strategy*, 12 December 2003, available at http://www.consilium.europa.eu/uedocs/cmsupload/78367.pdf.

[11] Justice and Home Affairs Council, *Internal Security Strategy for the European Union: Towards a European Security Model*, March 2010, available at www.consilium.europa.eu/uedocs/cms_data/librairie/PDF/QC3010313ENC.pdf.

[12] Council of the EU, *Council Conclusions on Migration*, Press Release 606/15, 20 July 2015, available at www.consilium.europa.eu/en/press/press-releases/2015/07/20-fac-migration-conclusions/.

[13] For the case of the conflict in Ukraine, see Council of the EU, *Statement of the Heads of State or Government*, Press Release 25/15, 27 January 2015, available at http://www.consilium.europa.eu/en/press/press-releases/2015/01/statement-of-the-heads-of-state-or-government/.

[14] See *Strategija sodelovanja RS v mednarodnih operacijah in misijah*, Uradni list RS no. 19/2010, 12 March 2010, available at https://www.uradni-list.si/1/content?id=96635.

[15] Richard L. Kugler, *Policy Analysis in National Security Affairs* (Washington D.C.: National Defense University Press, 2006), xv, 14.

[16] Steven B. Redd and Alex Mintz, "Policy Perspectives on National Security and Foreign Policy Decision Making," *Policy Studies Journal* 41, no. 1 (2013): 11-37, DOI: 10.1111/psj.12010.

[17] Ronald W. Perry and Michael K Lindell "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process," *Disasters* 27:4 (2003), 336-50, DOI: 10.1111/j.0361-3666.2003.00237.x.

[18] Justice and Home Affairs Council, *Internal Security Strategy for the European Union*.

[19] Council of the EU, *European Security Strategy*.

[20] For more on the broad approach in counter-terrorism, see Iztok, Prezelj, "Smart Counterterrorism: Incorporating the N-order Effects and Adopting a Human Security Perspective," *The Polish Quarterly of International Affairs* 22, no. 1 (2013), accessed on 22 August 2013, www.pism.pl/publications/journals/The_Polish_Quarterly_of_International_Affais/2013/1.

[21] Alessandro Politi, "European Security: The New Transnational Risks," *Chaillot Papers* 29 (1997), available at http://www.iss.europa.eu/publications/detail/article/european-security-the-new-transnational-risks/.

[22] Stephen M. Walt, "The Renaissance of Security Studies," *International Studies Quarterly* 35, no. 2 (June 1991), 211-39, DOI: 10.2307/2600471.

[23] Gwyn Prins, "The Four-Stroke Cycle in Security Studies," *International Affairs* 74, no. 4 (1998), 788; Terriff, Croft, James and Morgan, *Security Studies Today*.

[24] Sam Sarkesian, *US National Security: Policy Makers, Processes and Politics* (London: Lynne Reinner Publishers, 1995), 5.

[25] Buzan, *People, States and Fear*.

[26] Prezelj, "Challenges in Conceptualizing and Providing Human Security."

[27] Iztok Prezelj, Erik Kopač, Aleš Žiberna, Anja Kolak, and Anton Grizold, "Evolutionary Reality of the Policy of Revolution in Military Affairs: Results of a Comparative Study," unpublished paper, Research Project *Transforming Defence Policies in Contemporary Security Environment* (Ljubljana: University of Ljubljana, 2015).

[28] See Timothy Thomas, "Deciphering Asymmetry's Word Game," *Military Review* 81, no. 4 (July-August 2001): 32-37; Robert Worley, "Asymmetry and Adaptive Command," *Military Review* 81, no. 4 (July-August 2001): 38-44; Steven Metz, "Strategic Asymmetry," *Military Review* 81, no. 4 (July-August 2001): 23-31.

[29] Sun Tzu, *The Art of War* (Norwalk: The Puppet Press, 1910).

[30] National Commission on Terrorist Attacks Upon the United States, *9/11 Commission Report: The Full Final Report of the National Commission on Terrorist Attacks upon the United States* (Washington D.C., 2004), 399-428, available at www.9-11commission.gov/report/911Report.pdf.

[31] See Raphael Perl, *Terrorism and National Security: Issues and Trends* (Washington D.C.: Congressional Research Service, 2006), 15; Richard S. Conley, "Reform, Reorganization, and the Renaissance of the Managerial Presidency: The Impact of 9/11 on the Executive Establishment," *Politics & Policy* 34, no. 2 (2006): 324; Erik Brattberg, "Coordinating for Contingencies: Taking Stock of Post-9-11 Homeland Security Reforms," *Journal of Contingencies and Crisis Management* 20, no. 2 (2012): 86; Thomas H. Hammond, "Why is the Intelligence Community So Difficult to Redesign? Smart Practices, Conflicting Goals, and the Creation of Purpose-Based Organizations," *Governance: An International Journal of Policy, Administration, and Institutions* 20, no. 3 (2007): 421.

[32] Council of the EU, *Interim Report on the Evaluation of National Anti-Terrorist Arrangements*, 23 November 2004, available at www.consilium.europa.eu/uedocs/cmsUpload/Interim_Report.pdf.

[33] Daniel Nohrstedt and Dan Hansen, "Converging Under Pressure? Counterterrorism Policy Developments in the European Union Member States," *Public Administration* 88, no. 1 (2010): 190-210, DOI: 10.1111/j.1467-9299.2009.01795.x.

[34] Council of the EU, *The European Union Counter-Terrorism Strategy,* 30 November 2005, available at http://register.consilium.europa.eu/doc/srv?l=EN&f=ST+14469+2005+REV+4.

[35] Council of the EU, *Council Conclusions on Counter-terrorism*, Press Release 43/15, 9 February 2015, available at www.consilium.europa.eu/en/press/press-releases/2015/02/150209-council-conclusions-counter-terrorism/.

[36] Alan, Doig, "Joining Up a Response to Terrorism," *Crime, Law & Social Change* 44 (2005): 436, DOI:10.1007/s10611-006-9025-5.

[37] Bruce Hoffman, "Rethinking Terrorism and Counterterrorism Since 9/11," *Studies in Conflict & Terrorism* 25, no. 5 (2002): 314, DOI:10.1080/105761002901223.

[38] Rohan Gunaratna and Peter Chalk, *Counter-Terrorism* (Coulsdon: Jane's Information Group, 2002), 99; Paul R. Pillar, "Intelligence," in *Attacking Terrorism: Elements of a Grand Strategy,* ed. Audrey Kurth Cronin and James M. Ludes (Washington D.C.: Georgetown University Press, 2004), 115-39.

[39] Lindsay Cutterbuck, "Law Enforcement," in *Attacking Terrorism: Elements of a Grand Strategy,* ed. Audrey Kurth Cronin and James M. Ludes (Washington D.C.: Georgetown University Press, 2004), 140-61.

[40] Michael Sheehan, "Diplomacy," in *Attacking Terrorism: Elements of a Grand Strategy*, ed. Audrey Kurth Cronin and James M. Ludes (Washington D.C.: Georgetown University Press, 2004), 97-114.

[41] Timothy D. Hoyt, "Military Force," in *Attacking Terrorism: Elements of a Grand Strategy*, ed. Audrey Kurth Cronin and James M. Ludes (Washington D.C.: Georgetown University Press, 2004), 162-85.

[42] William L. Waugh, "Terrorism, Homeland Security and the National Emergency Management Network," *Public Organization Review* 3, no. 4 (2003): 373-85, DOI: 10.1023/B:PORJ.0000004815.29497.e5.

[43] Robert Bunker, "Introduction and Overview: Why Response Networks?" in *Networks, Terrorism and Global Insurgency,* ed. Robert Bunker (London, Routledge, 2005), 1-7; DOI: 10.1080/0966284042000279975.

[44] John P. Sullivan, "Networked All-Source Fusion for Intelligence and Law Enforcement Counter-terrorism Response" (paper presented at the ISA Annual Convention in Montreal, Canada, 2004), 1-11; John P. Sullivan and Robert Bunker, "Multilateral Counter-Insurgency Networks," in *Networks, Terrorism and Global Insurgency,* ed. Robert Bunker (London, Routledge, 2005), 184, DOI: 10.1080/0966284042000279081.

[45] Audrey Kurth Cronin, "Conclusion: Toward an Effective Grand Strategy," in *Attacking Terrorism: Elements of a Grand Strategy*, ed. Audrey Kurth Cronin and James M. Ludes (Washington D.C.: Georgetown University Press, 2004), 293.

[46] Bruce Hoffman, "A Counterterrorism Strategy for the Obama Administration," *Terrorism and Political Violence* 21 (2009), 369-70, DOI: 10.1080/09546550902950316.

[47] Erik Brattberg, "Coordinating for Contingencies: Taking Stock of Post-9-11 Homeland Security Reforms," *Journal of Contingencies and Crisis Management* 20, no. 2 (2012): 86, DOI: 10.1111/j.1468-5973.2012.00662.x.

[48] Sullivan and Bunker, "Multilateral Counter-Insurgency Networks," 189.

[49] Kurth Cronin, "Conclusion: Toward an Effective Grand Strategy," 293.

[50] Roderick M. Kramer, "A Failure to Communicate: 9/11 and the Tragedy of the Informational Commons," *International Public Management Journal* 8:3 (2005), 408-409, DOI: 10.1080/10967490500439867.

[51] Iztok Prezelj. "Role of the European Union in the Fight against International Terrorism," in *The Fight Against Terrorism and Crisis Management in the Western Balkans*, ed. Iztok Prezelj (Amsterdam: IOS Press, 2008), 16-34.

[52] Iztok Prezelj, "Improving Interorganisational Cooperation in Counterterrorism Based on a Quantitative SWOT Assessment," *Public Management Review*, 17, no. 1-2 (2015): 209-35, DOI: 10.1080/14719037.2013.792384.

[53] Myriam Dunn and Isabelle Wiegert, *International CIIP Handbook 2006: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, Volume 1 (Zurich: ETH – Swiss Federal Institute of Technology, 2006), accessed on 3 June 2014, www.e-collection.ethbib.ethz.ch/eserv/eth:31123/eth-31123-03.pdf.

[54] See Council of the EU, *Council Directive on the Identification and Designation of European Critical infrastructures and the Assessment of the Need to Improve their Protection*, 23 December 2008, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32008L0114.

[55] Gwendal Le Grand, Franck Springinsfeld and Michel Riguidel, *Policy Based Management for Critical Infrastructure Protection*, ACIP Project funded by the European Commission; Carmelo Di Mauro, Sara Bouchon, Christiaan Logtmeijer, Russell Pride, Thomas Hartung and Jean-Pierre Nordvik, "A Structured Approach to Identifying European Critical Infrastructures," *International Journal of Critical Infrastructures* 6, no. 3 (2010), DOI: 10.1504/IJCIS.2010.033340.

[56] Erwann Michel-Kerjan, "New Challenges in Critical Infrastructures: A US Perspective," *Journal of Contingencies and Crisis Management* 11, no. 3 (2003): 132-41, DOI: 10.1111/1468-5973.1103008; Philip Auerswald, Lewis Branscomb, Todd La Porte and Erwann

Michel-Kerjan, "The Challenge of Protecting Critical Infrastructure," *Issues in Science and Technology Fall* (2005), accessed on 8 June 2006, www.issues.org/22.1/auerswald.html.

[57] Ted Lewis, *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation* (New Jersey: Wiley Interscience, 2006).

[58] James Peerenboom, *Infrastructure Interdependencies: Overview of Concepts and Terminology*. Infrastructure Assurance Center, Argonne National Laboratory (Argonne: Wiley Interscience, 2001); Le Grand and Riguidel, *Policy Based Management for Critical Infrastructure Protection*; Thomas Hellstrom, "Critical Infrastructure and Systemic Vulnerability: Towards a Planning Framework," *Safety Science* 45, no. 3 (2007): 415-30, DOI: 10.1016/j.ssci.2006.07.007.

[59] Iztok Prezelj, Erik Kopač, Uroš Svete and Aleš Žiberna, "Cross-sectoral Scanning of Critical Infrastructures: From Functional Differences to Policy-relevant Similarities," *Journal of Homeland Security and Emergency Management* 9:1 (2012), accessed on 11 March 2013, DOI: 10.1515/1547-7355.1901.

[60] Richard Kugler, *Policy Analysis in National Security Affairs: New Methods for a New Era* (Washington, D.C., National Defense University Press, 2006); Mark de Bruijne, "Networked Reliability: Institutional Fragmentation and Critical Infrastructure Protection," Paper presented at the Conference on Future Challenges for Crisis Management in Europe, Stockholm, 4-5 May 2006; Mark Rhinard and Arjen Boin, "European Homeland Security: Bureaucratic Politics and Policymaking in the EU," *Journal of Homeland Security and Emergency Management* 6, no. 1 (2009); DOI: 10.2202/1547-7355.1480.

[61] See Myriam Dunn, "Analysis of Methods and Models for CII Assessment," in *International CIIP Handbook 2004*, ed. Myriam Dunn and Isabelle Wiegert (Zurich: ETH, 2004), 250-277, available at www.isn.ethz.ch/Digital-Library/Publications/Detail/?lang=en&id=472; Yacov Y. Haimes, "On the Complex Definition of Risk: A Systems-Based Approach," *Risk Analysis* 29, no. 12 (2009), 1647-54, DOI: 10.1111/j.1539-6924.2009.01310.x.

[62] European Commission, *Green Paper on a European Programme for Critical Infrastructure Protection,* EC COM(2005)576, 17 November 2005, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52005DC0576; The Council of the EU, *Proposal for a Directive of the Council on the Identification and Designation of European Critical Infrastructures*, 16933/06, 12 December 2006, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2006:0787:FIN:EN:HTML.

[63] See European Parliament and Council of the EU, Decision of the European Parliament and of the Council on a Union Civil Protection Mechanism, Official Journal of the EU, 20 December 2013, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32013D1313.

[64] Iztok Prezelj, "Matematično-statistični integralni model za ocenjevanje ogroženosti nacionalne varnosti in računalniški program INTEGRO," in *Model celovitega ocenjevanja ogrožanja nacionalne varnosti Republike Slovenije*, ed. Iztok Prezelj (Ljubljana: Ministrstvo za obrambo, 2007), 209-28.

Iztok PREZELJ is Associate Professor and Head of the Department of Defence Studies at the Faculty of Social Sciences, University of Ljubljana, Slovenia.
*E-mail*: iztok.prezelj@fdv.uni-lj.si.