International Relations and Diplomacy, Mar.-Apr. 2024, Vol. 12, No. 2, 72-85
doi: 10.17265/2328-2134/2024.02.004

Global and International Security Under Spatial Grasp Paradigm

Peter Simon Sapaty
National Academy of Sciences, Kyiv, Ukraine

Global and international security cannot be provided from a single point or a set of separate points whatever powerful these might be (even with quantum supercomputers!). It should rather be deeply embedded and integrated with bodies of real systems wherever in physical, virtual, or combined spaces they may exist. So global security capabilities should not only be distributed, but rather be really spatial, self-organized, and dynamic, also exhibiting overall integrity, awareness, and consciousness features. The paper describes applicability of the patented and revealed in 10 books Spatial Grasp Model and Technology (SGT) and its basic Spatial Grasp Language (SGL) which conceptually and functionally match security problems of large distributed and heterogeneous systems. It investigates very practical security solutions for finding and tracing distribution of forbidden items, world roaming criminals, recovery from natural and human-made disasters, tracing and elimination of moving dangerous objects in terrestrial and celestial spaces, as well as analysis and restoration of damaged transport networks. It advises how different security infrastructures can be organized and managed, and how to cooperate and integrate within global security systems with higher awareness and consciousness levels over them. The provided security-oriented version of SGL can be quickly implemented and integrated with existing distributed management and security systems.[1]

Keywords: global security, international security, critical infrastructures, Spatial Grasp Technology, Spatial Grasp Language, distributed language interpretation, self-recovering security scenarios, global security awareness and consciousness

1. Introduction

Paper's Goal

The main goal of this paper is to investigate what global security means, which problems need solutions for it both nationally and internationally, and then try to find and test a sort of unifying model and technology which could support world's security on its highest theoretical, organizational, technological, and mental levels.

Basic Definitions

We will be relying in the subsequent material on the following clear definitions, which are effectively supplementing each other.

Security, as by Wikipedia (2024a), is protection from, or resilience against, potential harm. Security mostly refers to protection from hostile forces, but it has a wide range of other senses like the absence of harm, presence of an essential good, resilience against potential damage or harm, secrecy, containment, and a state of mind. It can be physical and virtual.

Peter Simon Sapaty, Ph.D., Chief Research Scientist, Institute of Mathematical Machines and Systems, National Academy of Sciences, 42 Glushkov Avenue, 03187 Kyiv, Ukraine.

[1] "spatial grasp" in google.com.

Security, as in by Wikipedia (2024b) can also be freedom from danger, freedom from fear or anxiety, freedom from the prospect of being laid off job security, something given, deposited, or pledged to make certain the fulfillment of an obligation, an instrument of investment in the form of a document providing evidence of its ownership, measures taken to guard against espionage or sabotage, crime, attack, or escape, and so on.

International security, as from Wikipedia (2024c), is a term which refers to the measures taken by states and international organizations to ensure mutual survival and safety. These measures include military action and diplomatic agreements such as treaties and conventions. International and national security are invariably linked.

Global security, as in RAND (2024), includes military and diplomatic measures that nations and international organizations take to ensure mutual safety and security. It provides analyses that help policymakers understand political, military, and economic trends around the world, the sources of potential regional conflict, and emerging threats to the global security environment.

Organization of the Rest of the Paper

Section 2 is completely devoted to the existing global and international security publications. It starts with the security books, discusses examples of global security threats, provides a list of critical infrastructure sectors, also analyzes many other security oriented ideas and presentations. Section 3 briefs the key ideas and features of the Spatial Grasp Model and Technology (SGT) on which solutions presented in the book are based. These include general technology issues, its basic Spatial Grasp Language (SGL), and details of distributed and networked SGL interpreter organization. Section 4 provides examples of very practical security solutions, which include finding certain suspects worldwide, tracking and destruction of complexly moving hostile objects, and security swarm against enemy swarm elimination scenario. Section 5 shows examples of network infrastructure analysis and operations, which include finding strongest sub-networks or cliques of certain volumes, discovering weakest or articulation points in the infrastructures, and finding certain network structures using pattern matching techniques.

Section 6 provides and analyzes examples of combined infrastructure solutions, where the badly damaged road infrastructure activates for its emergency repair and improvement other critical infrastructure sectors like Terrain, Economy, Engineering, Employment, and so on. Section 7 concludes the paper with plans for deeper analysis and integration of critical infrastructures, where SGT, conceptually based or self-controlled, self-spreading, and self-recovering recursive code, can provide a potential breakthrough in this important global security area. References contain substantial publications on the security topics, and the model and technology investigated for security applications. The Appendix provides syntax and main constructs of SGL which may be particularly useful for the international and global security applications.

2. Global and International Security Publications

Numerous publications exist on this very important and diverse area and related topics, and will be starting below with security oriented books.

Security Books

Global Security (O'Connor, 2019) is about structures and processes that represent most serious threats on a planetary scale. It touches topics like armed conflict, transnational crime, cybersecurity, financial crisis, poverty, health, population dynamics, ecosecurity, natural and technological disasters, threats from outer space, and cultural hybridity.

Global Security in the Twenty-First Century (Kay, 2015) assesses the impact of the global economic crisis on international security and considers how the range of thinking about power and peace has evolved in relation to major world flashpoints. It emphasizes the roles of trade and technology, the militarization of space, the privatization of security, the use of sanctions, ethnic conflict, and transnational crime.

Understanding Global Security (Hough, 2018) analyses the variety of ways in which people's lives are threatened and/or secured in contemporary global politics. War, deterrence, and terrorism, are analyzed alongside non-military security issues such as famine, crime, disease, disasters, environmental degradation, and human rights abuses to provide a comprehensive survey of how and why people are killed in the contemporary world.

Artificial Intelligence and Global Security (Masakowski, 2020) presents a vision of a future that is replete with integrated networks of artificial intelligence that are designed to both defend and attack nations. It also explores the implications of AI for the individual, for personal identity, for society, and for global security; and offers diverse perspectives on the consequences of the integration of AI in our daily lives and society.

Global Security Upheaval (Mandel, 2013) reveals that areas exist where it makes little sense to rely on state governments for stability, and that attempts to bolster such governments to promote stability often prove futile. It demonstrates how armed non-state groups can sometimes provide local stability better than states, and how power-sharing arrangements between states and armed non-state groups may sometimes be viable.

The Oxford Handbook of International Security (Gheciu & Wohlforth, 2020) is on the state of international security and the academic field of security studies. The topics covered range from conventional international security themes such as arms control, alliances, and Great Power politics, to "new security" issues such as global health, the roles of non-state actors, cyber-security, and the power of visual representations in international security.

International Security: Problems and Solutions (Morgan, 2006) progresses from negotiation and mediation to peace imposition. It evaluates each strategy and tactic in terms of how well it addresses three levels of security—systemic, state, and societal—to show how they are interrelated and complementary to each other in important ways. Addressing insecurity at one level often elicits further insecurity at another.

International, and Human Security: Protection against Violence (Neack, 2023) provides a thorough overview of how states pursue security against violence, and how this pursuit paradoxically creates greater insecurity at the national, international, and individual levels. The traditional insistence that states are the primary and most important actors makes security, ultimately, elusive.

Examples of Global Threats

Some of the biggest threats to international security we face on a global scale, may be as follows (just as mentioned by Universidad Europea (2024)), and there may be many more.

- *Terrorism*: Global terrorism is an unfortunate reality of modern times. These indiscriminate and targeted acts can come from a range of terrorist organizations, small groups, or individuals.
- *Climate change*: Extreme weather is becoming increasingly common as the world gets warmer: recurrent droughts, violent wind, and fire storms, rising sea levels, also threat of new disease outbreaks.
- *Conflict and war*: There are now more active conflicts than any time since 1945. Globally, there are now more than 82 million people living in refugee and displacement camps or far from home.
- *Hunger and malnutrition*: The threat of hunger now faces 45 million people in 43 countries around the world. Millions of people are living on the brink of starvation and urgently need food to survive.
- *Artificial intelligence*: While AI has its positives in many processes, there are also numerous concerns about it, as the misuse of AI may result in spreading false information of all sorts.

Examples of Security-Related Critical Infrastructures

The term *Critical Infrastructures* (Moulos et al., 2018) describes the assets that are vital for a society to function correctly. Critical infrastructures provide the essential services that underpin society and serve as the backbone of the global economy, national security, and the public health sector. The main critical infrastructure sectors may include the following (as mentioned by Moulos et al. (2018)): Chemical Sector, Commercial Facilities Sector, Communications Sector, Critical Manufacturing Sector, Defense Industrial Base Sector, Emergency Services Sector, Energy Sector, Financial Services Sector, Food and Agriculture sector, Government Facilities Sector, Healthcare and Public Health Sector, Information Technology Sector, Nuclear Reactors Sector, Materials and Waste Sector, Transportation Systems Sector, Water and Wastewater Systems Sector.

Other Security Oriented Publications

We have studied and analyzed many more security-oriented sources and publications which proved very useful for the developing material of this paper, including: IGI Global (2024); Sherman (1992); Xiao & Pan (2007); Rowan University (2024); Check Point (2024); NordLayer (2024); Alpha Media LLC (2024); Prynne (2014); U.S. News (2024); Schneier (2008); Chitadze (2022); University of St Andrews (2024); Cottam, Mastors, Preston, & Dietz (2022); Safdar, Akhtar, Baig, & Ahamad (2022); Butcher (2018); Davis (2012); Ganame, Bourgeois, Bidou, & Spies (2008); Rinaldi, Peerenboom, & Kelly (2002). They are covering the following areas and topics: Distributed Security, Distributed Systems Security, Security in Distributed and Networking Systems, Global Security Problems, What is Network Security, Network security: everything you need to know, Sophisticated Criminal Groups, Foreign criminals roaming Britain's streets, Illegal border Crossings from Mexico, The Psychology of International Security, The Political Psychology of International Security and Conflict, Global Security and Human Rights, Role of research psychology in defense and security, Psychology, Strategy and Conflict, Global Security Architecture for Intrusion Detection, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.

3. Spatial Grasp Model and Technology

Only most general features of the developed paradigm are mentioned here, with availability of existing extended publications on its philosophy, features, organization, and numerous applications, including Sapaty (1993; 1999; 2005; 2017; 2018; 2019; 2021; 2022; 2023a; 2023b; 2023c; 2023d; 2023e; 2023f; 2023g; 2024a; 2024b).

General Issues

Within Spatial Grasp Model and Technology (SGT), a high-level operational scenario expressed in recursive Spatial Grasp Language (SGL), starting in any world point, *propagates, covers, and matches the distributed environment in parallel wavelike mode*, as symbolically shown in Figure 1. Such propagation can result in returning and analyzing the reached states and data which may be arbitrarily remote, or used for launching more waves.

The distributed worlds this model effectively covers, conquers, and manages may be of different types: *Physical World (PW)* considered as continuous and infinite where each point can be identified and accessed by physical coordinates; *Virtual World (VW)* which is discrete and consists of nodes and semantic links between them, and *Executive World (EW)* consisting of active doers, which may be humans or robots with communication possibilities between them. Different kinds of combinations of these worlds can also be possible within the same formalism.

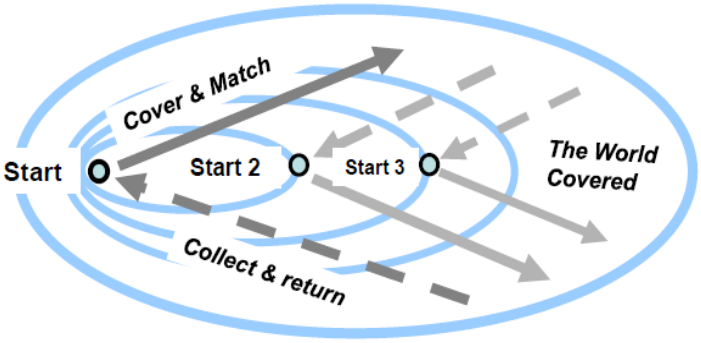


Figure 1. Parallel recursive world coverage with Spatial Grasp Model.

Spatial Grasp Language (SGL)

The SGL allows for direct space presence and operations with unlimited powers and parallelism. Its universal recursive organization, with operational scenarios called *grasp*, can be expressed by a single formula:

grasp → *constant* | *variable* | *rule* ({ *grasp*, })

The *rule* can express certain action, control, description, or context accompanied with operands, which can be any *grasps* too. Other top SGL details can be expressed as:

constant → *information* | *matter* | *custom* | *special*

variable → *global* | *heritable* | *frontal* | *nodal* | *environmental*

rule → *type* | *usage* | *movement* | *creation* | *echoing* | *verification* | *assignment* | *advancement* | *branching* | *transference* | *exchange* | *timing* | *qualifying*

The rules, starting in certain points, can organize navigation of the world sequentially, in parallel, or any combinations thereof. They can result in the same application points or cause movement to other world points with obtained results left there or returned. The final points reached can become starting ones for other rules. The rules, due to recursive language organization, can form *arbitrary operational infrastructures* expressing sequential, parallel, hierarchical, centralized, up to fully decentralized, and distributed algorithms. Details of the latest SGL version are summarized in the Appendix.

SGL Interpreter Organization

The SGL interpreter consists of specialized modules working with specific data structures, serving SGL scenarios or their parts happened to be within this interpreter, also organizing exchanges with other interpreters for distributed SGL scenarios. Each interpreter copy can process multiple active scenario code propagating in space and time. Communicating SGL interpreters can be in arbitrary number of copies effectively integrated with other existing systems and communications, representing altogether *powerful spatial engines operating without central resources or control*. Hardware or software SGL interpreters, shown in Figure 2 as universal control and processing units effectively working with spatial graph and network data, can be installed, runtime created too, in proper physical or virtual world points.

As both backbone and nerve system of the distributed interpreter, its self-optimizing *Spatial Track System* provides hierarchical command and control, also remote data and code access. It supports spatial variables, some of which can be mobile, and merges distributed control states for making decisions at different organizational levels. This spatial infrastructure, effectively supporting global integrity of distributed solutions, is automatically distributed between active components (humans, robots, computers, smart-phones, satellites, etc.) during SGL scenario self-evolution in space and time.

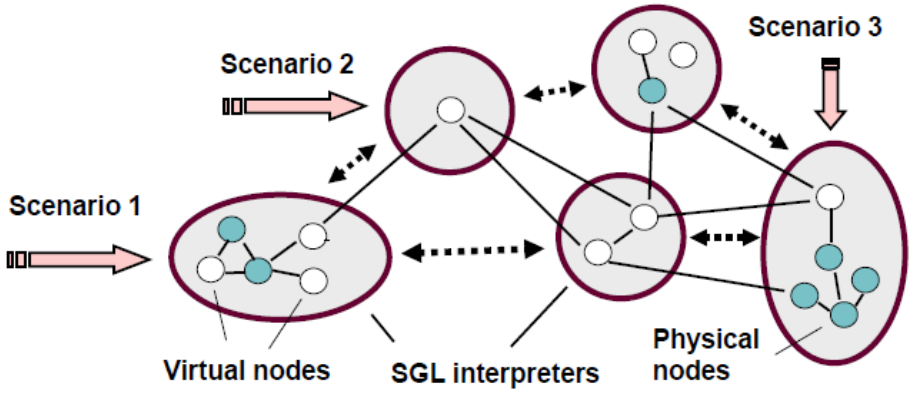


Figure 2. SGL distributed networked interpretation.

4. Examples of Practical Security Solutions

Finding Suspects Worldwide

Imagine we have to find information about individuals indentified by specific Features while originating in some START position. When staying in START, the individuals may be found by a match of Features with local_databases. The latter may not have records on all individuals sought, but their traces may exist in some local_security systems. If such exists and leads to other locations, we may search there too, and so on. The found match from different world points can be collected, returned to START, and output by the following SGL scenario, see also Figure 3.

```
frontal(Features) = …; nodal(Other);
hopfirst(START);
output(repeat(free(match(Features, local_databases)),
                Other = traces(Features, local_security);
                hopfirst(Other)))
```

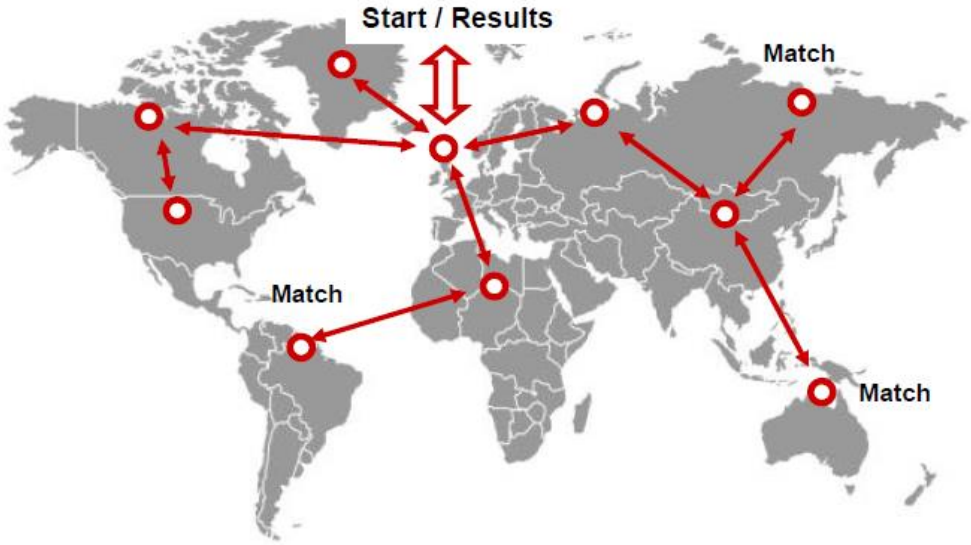


Figure 3. Worldwide search for suspects with the return of matching found.

Answer in the START point may be as follows:

match_1, match_2, …, match_m

Tracking Mobile Objects

The following self-evolving spatial scenario discovers and tracks hostile objects propagating through the distributed area equipped with a network of radar-battery stations, as in Figure 4. The complexly moving objects are constantly controlled by the spatial intelligence self-spreading between stations, which also collects, updates, and analyses history of their behavior, and if needed, commands their destruction.

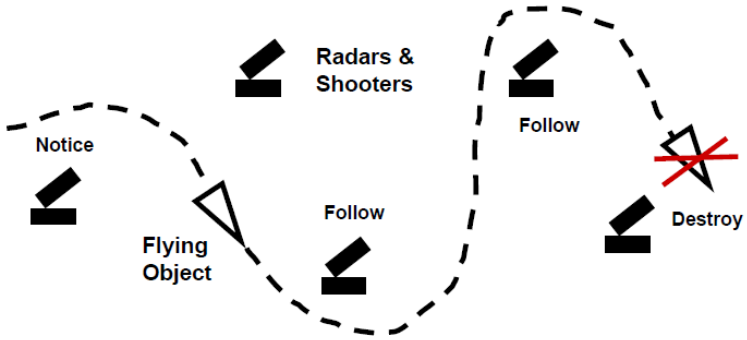


Figure 4. Tracking mobile objects with mobile spatial intelligence.

```
hop(all_nodes); frontal(Object, History);
whirl(
   Object = search(aerial, new);
   visibility(Object) > threshold;
   repeat(
      loop(visibility(Object) > Threshold; update(History));
            If(negative(History), quit(destroy(Object))));
      max_destination(hop(all_neighbors); visibility(Object));
      visibility(Object) > threshold)))
```

Swarm Against Swarm Scenario

This scenario describes an unmanned swarm of security vehicles, called Chasers, which are discovering and chasing a group of unwanted objects (like explosive or spying drones, which may operate as swarms too), see also Figure 5. Each chaser seeing some targets informs other chasers about their positions, and tries to select the nearest target to follow and destroy individually. If all targets are still far away to shoot them, chasers are just moving towards the center of hostile group unless they become close to a target to shoot.

```
frontal(Targets); nodal(All, Nearest);
hop(all_chasers);
repeat(
   collect_visible(Targets, Threshold1);
   free(hop(all_chasers); update(All, Targets));
   Nearest = min_distance(WHERE, All);
   If(Nearest < Threshold2, follow_destroy(Nearest));
   orient_step_toward(average(All)))
```

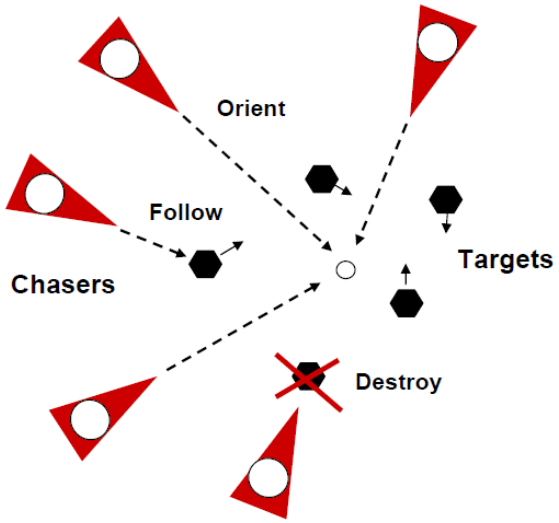


Figure 5. Chasing and destroying hostile targets.

5. Examples of Infrastructure Network Operations

More complex distributed operations and solutions may be needed when dealing with complex and networked security infrastructures, with only a few examples mentioned in this section.

Finding Strongest Sub-networks, or Cliques

We present here a universal solution in SGL for finding cliques in the network (*maximum full sub-graphs* of certain qualities and volumes), which may reflect, for example, strong criminal or security groupings distributed over large spaces. The following scenario is finding all cliques in the network, like of Figure 6, with the number of nodes not less than three (only a clique with four nodes is highlighted in the figure).

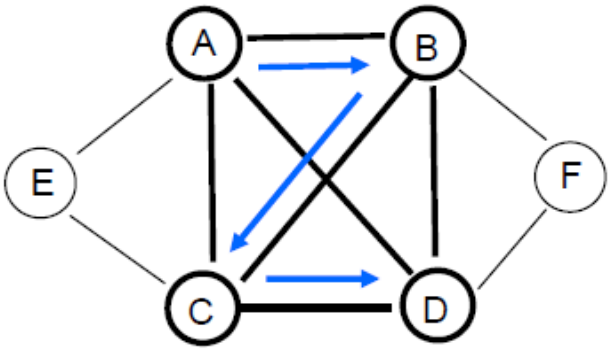


Figure 6. Finding strongest parts, or cliques, in the network.

```
hop_nodes(all); frontal(Clique) = NAME;
repeat(
   hop_links(all); not_belong(NAME, Clique);
   yes(and_parallel(hop(links_any, nodes(Clique))));
   if(PREDECESSOR > NAME, append(Clique, NAME), blind));
count(Clique) >= 3; output(Clique)
```

The obtained full results for Figure 6 will be: (A,B,C,D), (A,C,E),(B,D,F).

Discovering Weakest, or Articulation Points

Weakest or articulation points, when removed, split the network into disjoint parts, like node E in Figure 7, which may weaken the whole systems dramatically (whether criminal or on the opposite security one).

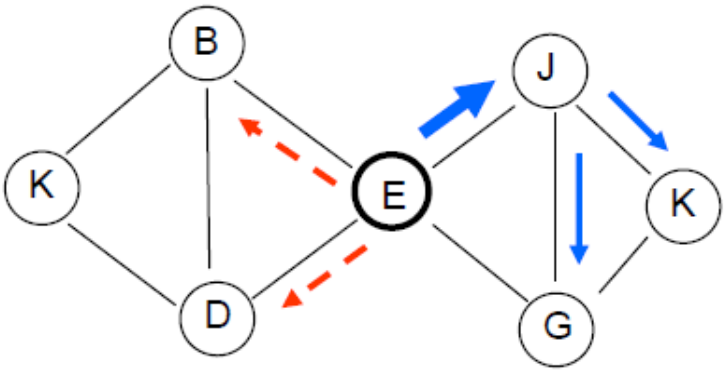


Figure 7. Weakest, or articulation point of the network.

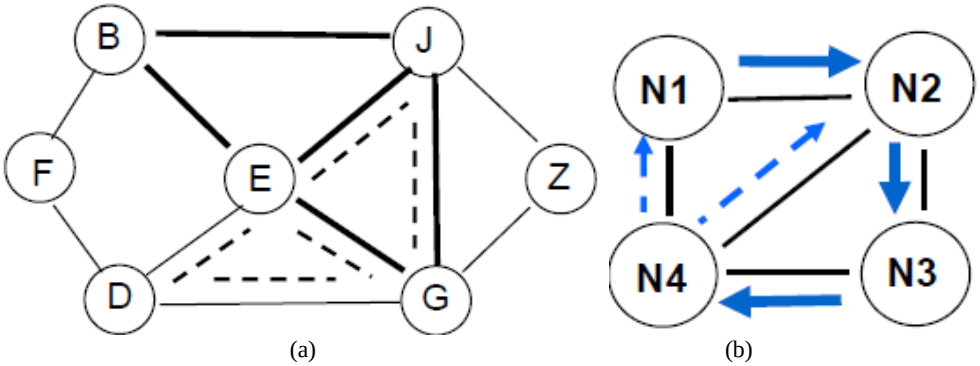
Next is parallel and fully distributed solution for finding all articulation points in the network, by which each network node, first selecting one neighbor randomly, tries to navigate and mark the whole network from it while excluding itself from this process. After the termination, if the node discovers still unmarked neighbors, it declares itself articulation point, as follows:

```
hop_nodes(all); IDENTITY = NAME;
hopfirst_node(current);
stay(hopfirst_random(links_all);
      repeat(hopfirst(links_all)));
if(hopfirst(links_all), output(NAME))
```

The answer for Figure 7 will be the only node E.

Network Pattern Matching

Finding specific network structures may represent another important tasks and solutions in security infrastructures. As an example, we will be trying to find in the network of Figure 8a, a structure described by a pattern of connected nodes of Figure 8b. Among possible matching techniques may be the one based on a path through all pattern's nodes, as shown min blue in Figure 8b. The SGL self-matching scenario may be as follows.



(a) (b)

Figure 8. (a) Distributed network, (b) Pattern to be matched.

```
hop_nodes(all); frontal(Nodes) = NAME;
three_repeat(hop_link(all); notbelong(NAME, Nodes); Nodes && = NAME);
true(andparallel(link(any), Nodes[1,2]));
output(Nodes)
```

It will provide tree matching results (B, E, J, G), (D, E, J, G), and (E, J, G, Z); only first two are highlighted in Figure 8a. Removing any found matching from the network (which, for example, may happen to be extremely dangerous) can be easily done by substituting the final operation output(Nodes) with remove(Nodes).

6. Example of Combined Infrastructure Solutions

Damaged Roads Situation

Imagine in the road network of Figure 9 that node 12 together with roads to nodes 4 and 8 was accidentally damaged or even destroyed (say, by being bombed), and we need to find the shortest route from node 1 to node 11 (which was definitely via node 12 before). The following SGL scenario will be finding the new shortest route from 1 to 12 (say, as shown in Figure 9 in blue).

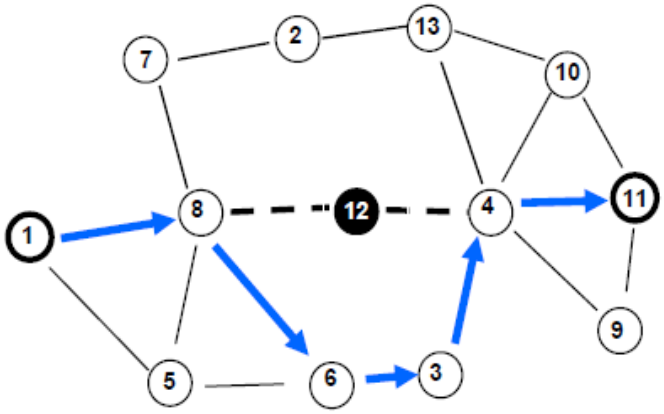


Figure 9. Finding a new route in the damaged transport infrastructure.

```
nodal(Dist, Up); frontal(Far);
sequence(
(hop(1); Dist = 0;
repeat(hop(links_all); Far += length(passed_link);
        or(Dist == nil, Dist > Far);
        Dist = Far; Up = BACK)),
(hop(11); frontal(Path);
repeat(Path = append(NAME, Path); hop(Up));
output(Path)))
```

The reply will be: (1, 8, 6, 3, 4, 11).

Infrastructures Cooperation and Integration Example

To repair this road network, also add, for safety, some additional roads from the recovered node 12 (like to nearest to it nodes 2, 3, 6, and 13), we have to request other critical infrastructure security sectors like Terrain and Economy (other infrastructures may need their involvement too), and investigate existing possibilities to accomplish these repairs and extensions, as follows, see also Figure 10.

Request = roads_needed(from 12 to(8, 2, 13, 4, 3, 6));

hop(Terrain, Economy); activate(Request)

The received combined Terrain-Economy reply may be as follows (see also Figure 10, in blue):

Roads possible from 12 to (8, 13, 4, 6).

To physically implement this result we will definitely have to contact other critical infrastructure sectors, and first of all, Engineering and Employment ones, which should also be tightly cooperating with the Economy sector, as follows, see also Figure 10:

hop(Engineering, Employment); create_roads(from 12 to (8, 13, 4, 6))

Other local and global infrastructures may also be engaged to execute and complete this request, and more cooperation should be organized with and between the already mentioned ones.

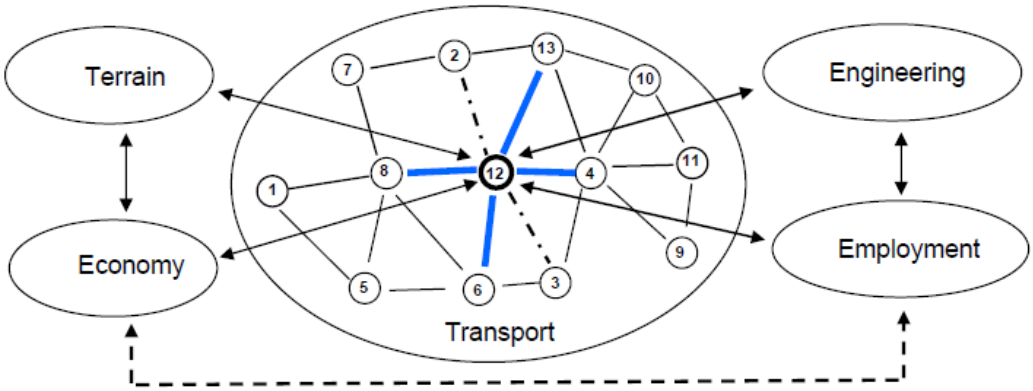


Figure 10. Interplay of critical infrastructures for solving emergent transport problem.

7. Conclusions

We have shown only a few practical examples of how SGT can be used for solving different security problems appearing on both national and international levels. These included local solutions for eliminating different threats and repairing after casual damages, also more global operations on the level of critical infrastructures which are based on distributed networks. In previous publications on this model and technology (including: Sapaty, 1999; 2005; 2017; 2018; 2019; 2021; 2022; 2023a; 2023b; 2023c; 2023d; 2023e; 2023f; 2023g; 2024a; 2024b) many more solutions of security-related problems were investigated (like global protection from deadly viruses, evacuation from disaster zones, advanced battlefield scenarios, fighting flooding and forest fires, removing space debris, basic distributed graph and network operations, and many others). All these confirm that international and global security is not only distributed, but has really *spatial nature*. And the developed *spatial grasp* paradigm providing effective supervision and control over any physical and virtual spaces can effectively fit these global protection and security goals. Operating as a powerful ubiquitous self-evolving and self-matching flooding, or even super-virus (*which cannot be destroyed even in principle due to effective self-recovery features*), it has a simple implementation which can be accomplished by a small group of system programmers and integrated with other communication and networking infrastructures (as was done and tested for the previous versions). The next plans of this research include investigation of SGT for a much wider repertoire of security tasks on a global international level, also deep integration of critical infrastructures with introduction superior psychological and consciousness-like security features, as symbolically shown in Figure 11. A new global security oriented book using ideas of this paper is also planned.

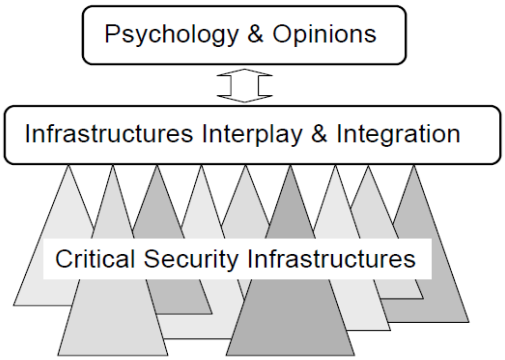


Figure 11. Hypothetical organization of advanced global security systems.

References

Alpha Media LLC. (2024). "Sophisticated criminal groups" roaming the desert, ready to attack…you. Retrieved from https://www.knewsradio.com/sophisticated-criminal-groups-roaming-the-desert-ready-to-attack-you/

Butcher, F. (2018). Role of research psychology in defence and security. Retrieved from https://militaryhealth.bmj.com/content/165/2/113

Check Point. (2024). What is network security? Retrieved from https://www.checkpoint.com/cyber-hub/network-security/what-is-network-security/

Chitadze, N. (2022). World politics and the challenges for international security. Retrieved from https://www.igi-global.com/book/world-politics-challenges-international-security/279369

Cottam, M. L., Mastors, E., Preston, T., & Dietz, B. (2022). The political psychology of international security and conflict. London: Routledge. Retrieved from https://www.taylorfrancis.com/chapters/mono/10.4324/9780429244643-13/political-psychology-international-security-conflict-martha-cottam-elena-mastors-thomas-preston-beth-dietz

Davis, J. W. (Ed.). (October 1, 2012). *Psychology, strategy and conflict: Perceptions of insecurity in international relations (Routledge global security studies).* London: Routledge. Retrieved from https://www.amazon.in/Psychology-Strategy-Conflict-Perceptions-International/dp/0415622042

Ganame, A. K., Bourgeois, J., Bidou, R., & Spies, F. (2008). A global security architecture for intrusion detection on computer networks. *Computers & Security*, *27*(1-2), 30-47. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/S0167404808000047

Gheciu, A., & Wohlforth, W. C. (August 4, 2020). *The Oxford handbook of international security.* Oxford: Oxford University Press.

Hough, P. (March 27, 2018). *Understanding global security* (4th ed.). London: Routledge.

IGI Global. (2024). What is distributed security? Retrieved from https://www.igi-global.com/dictionary/blockchain-for-transformation-in-digital-marketing/102330

Kay, S. (March 6, 2015). *Global security in the twenty-first century: The quest for power and the search for peace* (3rd ed.). Lanham, MD: Rowman & Littlefield Publishers.

Mandel, R. (April 3, 2013). *Global security upheaval: Armed nonstate groups usurping state stability functions* (1st ed.). Stanford: Stanford University Press.

Masakowski, Y. R. (July 15, 2020). *Artificial intelligence and global security: Future trends, threats and considerations*. Bingley: Emerald Publishing Limited.

Morgan, P. M. (February 27, 2006). *International security: Problems and solutions* (1st ed.). Washington, DC: CQ Press.

Moulos, V., Chatzikyriakos, G., Kassouras, V., Doulamis, A., Doulamis, N., Leventakis, G., …, Gatzioura, A. (2018). A robust information life cycle management framework for securing and governing critical infrastructure systems. *Inventions, 3*(4), 71. Retrieved from https://doi.org/10.3390/inventions3040071

Neack, L. (April 11, 2023). *National, international, and human security: Protection against violence* (3rd ed.). Lanham: Rowman & Littlefield Publishers.

NordLayer. (2024). Network security: Everything you need to know. Retrieved from https://nordlayer.com/learn/network-security/what-is-network-security/

O'Connor, T. R. (January 14, 2019). *Global security.* Solana Beach, CA: Cognella Academic Publishing.

Prynne, M. (February 24, 2014). More than 750 foreign criminals roaming Britain's streets. Retrieved from https://www.telegraph.co.uk/news/uknews/law-and-order/10657400/More-than-750-foreign-criminals-roaming-Britains-streets.html

RAND. (2024). Global security. Retrieved from https://www.rand.org/topics/global-security.html

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2002). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems, 21*(6), 11-25. doi:10.1109/37.969131

Rowan University. (2024). Global security problems. Retrieved from https://chss.rowan.edu/centers/inter_majors/interdisciplinary_programs/internationalstudies/global_security_resource/global-security-problems.html

Safdar, M. A., Akhtar, N., Baig, K., & Ahamad, W. (2022). Global security and human rights. *Journal of Positive School Psychology, 6*(10), 867-874. Retrieved from https://journalppw.com/index.php/jpsp/article/view/13207/8577

Sapaty, P. S. (1993). A distributed processing system. European Patent N 0389655, Publ. 10.11.93, European Patent Office.

Sapaty, P. S. (1999). *Mobile processing in distributed and open environments*. New York: John Wiley & Sons.

Sapaty, P. S. (2005). *Ruling distributed dynamic worlds*. New York: John Wiley & Sons.

Sapaty, P. S. (2017). *Managing distributed dynamic systems with spatial grasp technology*. New York: Springer.

Sapaty, P. S. (2018). *Holistic analysis and management of distributed social systems.* New York: Springer.

Sapaty, P. S. (2019). *Complexity in international security: A holistic spatial approach*. Bingley: Emerald Publishing.

Sapaty, P. S. (2021). *Symbiosis of real and simulated worlds under spatial grasp technology*. New York: Springer.

Sapaty, P. S. (2022). *Spatial grasp as a model for space-based control and management systems*. Boca Raton: CRC Press.

Sapaty, P. S. (2023a). *The spatial grasp model: Applications and investigations of distributed dynamic worlds*. Bingley: Emerald Publishing.

Sapaty, P. S. (2023b). Spatial management of air and missile defence operations. *Mathematical Machines and Systems, 6*(1), 30-49. Retrieved from http://www.immsp.kiev.ua/publications/articles/2023/2023_1/01_23_Sapaty.pdf

Sapaty, P. S. (2023c). Providing distributed system integrity under spatial grasp technology. *Mathematical Machines and Systems, 6*(2), 18-27. Retrieved from http://www.immsp.kiev.ua/publications/articles/2023/2023_2/02_23_Sapaty.pdf

Sapaty, P. S. (2023d). Providing global awareness in distributed dynamic systems. *International Relations and Diplomacy, 11*(2), 87-100. doi:10.17265/2328-2134/2023.02.002. Retrieved from https://www.davidpublisher.com/Public/uploads/Contribute/6486c3d05a6cc.pdf

Sapaty, P. S. (2023e). Simulating distributed consciousness with spatial grasp model. *Mathematical Machines and Systems, 6*(3), 13-30.

Sapaty, P. S. (2023f). Network centrality operations under spatial grasp technology. *Journal of Advances in Artificial Intelligence and Machine Learning, 1*(1), 1-11. Retrieved from https://www.scivisionpub.com/journals/articleinpress-journal-of-advances-in-artificial-intelligence-and-machine-learning

Sapaty, P. S. (2023g). Managing distributed systems with spatial grasp patterns. *Mathematical Machines and Systems, 6*(4), 11-25. Retrieved from http://www.immsp.kiev.ua/publications/articles/2023/2023_4/04_23_Sapaty.pdf

Sapaty, P. S. (2024a). *Providing integrity, awareness, and consciousness in distributed dynamic systems.* Boca Raton: CRC Press.

Sapaty, P. S. (2024b). *Spatial networking in the united physical, virtual, and mental world.* New York: Springer. Retrieved from https://www.amazon.com/Spatial-Networking-Physical-Virtual-Decision/dp/3031621530/

Schneier, B. (June 2008). The psychology of security. *Communications of the ACM, 50*(5), 50-79. Retrieved from https://www.researchgate.net/publication/221462155_The_Psychology_of_Security

Sherman, R. L. (March 1992). Distributed systems security. *Computers & Security, 11*(1), 24-28. Retrieved from https://www.sciencedirect.com/science/article/abs/pii/016740489290216E

U.S. News. (January 27, 2024). Illegal border crossings from Mexico reach highest on record in December before January lull. Retrieved from https://apnews.com/article/immigration-border-crossings-mexico-biden-18ac91ef502e0c5433f74de6cc629b32

Universidad Europea. (2024). International security threats—What are the main ones? Retrieved from https://universidadeuropea.com/en/blog/international-security-threats/

University of St Andrews. (2024). IR4546: The psychology of international security, Academic year(s): 2018-2019. Retrieved from https://portal.st-andrews.ac.uk/catalogue/View?code=IR4546&academic_year=2018%2F9

Wikipedia. (2024a). Security. Retrieved from https://en.wikipedia.org/wiki/Security

Wikipedia. (2024b). Security. Retrieved from https://www.merriam-webster.com/dictionary/security

Wikipedia. (2024c). International security. Retrieved from https://en.wikipedia.org/wiki/International_security

Xiao, Y., & Pan, Y. (Eds.). (August 2007). Security in distributed and networking systems. Retrieved from https://www.worldscientific.com/worldscibooks/10.1142/6513#t=aboutBook

Appendix: Updated Summary of SGL Syntax and Main Constructs

Syntactic categories are shown below in italics, vertical bar separates alternatives, parts in braces indicate zero or more repetitions with a delimiter at the right, and constructs in brackets are optional. The remaining characters and words are the language symbols (including boldfaced braces).

grasp	→	*constant* | *variable* | [*rule*] [({ *grasp*,})]
constant	→	*information* | *matter* | *special* | *custom* | *grasp*
information	→	*string* | *scenario* | *number*
string	→	‘{*character*}’
scenario	→	**{**{*character*}**}**
number	→	[*sign*]{*digit*}[.{*digit*}[e[*sign*]{*digit*}]]
matter	→	“{*character*}”
special	→	thru | done | fail | fatal | infinite | nil | any | all | other | all other | current | passed | existing | neighbors | direct | forward | backward | synchronous | asynchronous | virtual | physical | executive | engaged | vacant | first come | unique
variable	→	*global* | *heritable* | *frontal* | *nodal* | *environmental*
global	→	G{*alphameric*}
heritable	→	H{*alphameric*}
frontal	→	F{*alphameric*}
nodal	→	N{*alphameric*}
environmental	→	type | name | content | address | qualities | where | back | previous | predecessor | doer | resources | link | direction | thru | when | time | state | value | identity | in | out | status
rule	→	*type* | *usage* | *movement* | *creation* | *echoing* | *verification* | *assignment* | *advancement* | *branching* | *transference* | *exchange* | *timing* | *qualifying* | *grasp*
type	→	global | heritable | frontal | nodal | environmental | matter | number | string | scenario | constant | custom
usage	→	address | coordinate | content | index | time | speed | name | place | center | range | doer | node | link | unit
movement	→	hop | hop first | hop forth | move | shift | follow
creation	→	create | linkup | delete | unlink
echoing	→	state | rake | order | unit | unique | sum | count | first | last | min | max | random | average | sort up | sort down | reverse | element | position | from to | add | subtract | multiply | divide | degree | separate | unite | attach | append | common | withdraw | increment | decrement | access | invert | apply | location | distance
verification	→	equal | non equal | less | less or equal | more | more or equal | bigger | smaller | heavier | lighter | longer | shorter | empty | nonempty | belong | not belong | intersect | not intersect | yes | no
assignment	→	assign | assign peers
advancement	→	advance | slide | repeat | align | fringe
branching	→	branch | sequence | parallel | if | or | and | or sequence | or parallel | andsequence | andparallel | choose | quickest | cycle | loop | sling |whirl | split | replicate
transference	→	run | call
exchange	→	input | output | send | receive | emit | get
timing	→	sleep | allowed
qualification	→	contain | release | trackless | free | blind | quit | abort | stay | lift | seize | exit