e-Networks in an Increasingly Volatile World
Proceedings of the 11th International Workshop on Telework
August 28 – 31, 2006

Use of Anti-Terrorist Digital Ecosystem in the Fight Against Terrorism

Maja HADZIC and Elizabeth CHANG
Curtin University of Technology, School of Information Systems, Australia

Maja.Hadzic@cbs.curtin.edu.au

Abstract: In this chapter, we propose an Anti-terrorist Digital Ecosystem (ATDES) that enables efficient terrorist identification and protection against terrorist attacks. An Anti-terrorist Digital Environment (ATDE) is designed as being populated by interconnected Anti-terrorist Digital Components (ATDC). ATDC are combined together to support collaboration, cooperation and sharing of available information between various regions, countries and even continents.
ATDC may be any useful idea that can be digitalized, transported within the ecosystem and processed by humans or by computers. The key ATDC include ID databases that contain personal records, screening components that read personal records and match them with the available information from the ID databases and machine-readable personal records. The available information is put into one big virtual database and enables matching of personal records.
If the available information is to be shared between various ID information resources, standardization of data needs to take place. Ontologies can be used for this purpose. Instantiation of the Ontology concepts result in ID Ontologies that act as personal records. Because Ontology files are machine readable, it is possible to do the matching of personal records with the available ID records from the networked ID databases and to action the results.
The significance of this research lies in the unification of the advances of the Ontology technology and Ecosystem paradigm for the purpose of creating a more secure environment in which to fight against terrorism.

Keywords: Anti-terrorism, Digital Ecosystem, Digital Environment, Digital Components, Ontology.

Introduction

Every day we are surrounded by and face problems associated with terrorist attacks. People live in fear and insecurity. This situation is unnecessary as it does not solve any problems. Moreover, it brings forth only corruption of lives and families.

People are trying to establish an active anti-terrorist community and communication routes as they are working towards the same goal. An advertisement calling against terrorism in Australia bears the title: 'Every piece of information helps'. But, how do we

A. Gaudes (ed.)
University of New Brunswick
ISBN 1-55131-107-0

determine the crucial information? There is a need to find a way to enable this crucial piece of information to be as efficiently as possible, added to the information system, processed within the system and acted upon when needed. The system needs to be designed to support collaboration and cooperation as well as sharing of the available information between various regions, countries and even continents. A support network needs to be designed that provides the knowledge and resources as well as enables dynamic interconnections among various anti-terrorist organizations.

We aim to create a software infrastructure that will enable optimal use of the available information and support efficient knowledge sharing between various organizations for the purpose of efficient identification of terrorist groups or individuals. This infrastructure will allow linking of information resources into an organizational network. In this way, information becomes easily accessed and adapted to local needs. Digital Ecosystem provides the framework which allows organizations to collaborate and promotes local and global cooperation. We aim to establish an anti-terrorist community that is supported by a strong foundation of globally interacting anti-terrorist organizations that are moving towards shared vision and are able to find mutually supportive roles.

1. Digital Ecosystem

A Digital Ecosystem is composed of various Digital Components where each Digital Component has its uniquely assigned function. Digital Components together with a Digital Environment form a Digital Ecosystem. Those Digital Components are organized and connected to each other in a way that enables the Digital Ecosystem to function most effectively. Some of those Digital Components are more important than others. Some Digital Components are crucial for the existence of the Digital Ecosystem, while others are not so important and the Digital Ecosystem can still function without them. In the nature, plants, animals, fungi and microbial organisms are living parts of an ecosystem while the physical surroundings such as minerals found in the soil are known as environment or habitat. Digital Components are analogous with plants, animals, fungi and microbial organisms while the Digital Ecosystem is analogous to the ecosystem. A Digital Environment is analogous to environment or habitat.

A Digital Ecosystem captures the essence of the classical complex ecological community in nature. Digital Organisms (such as software or database applications, analogous to biological organisms) together with a Digital Environment (analogous to the biological environment) form a dynamic and interrelated complex Digital Ecosystem. A Digital Ecosystems transpose mechanisms from living organisms like evolution, adaptation, autonomy, viability and self-organization to arrive at novel knowledge and architectures [1].

Digital Ecosystem is a dynamic, complex and adaptive system composed of interrelated parts. It interacts with its environment and is subject to resulting feedback effects. A Digital Ecosystem evolves over time adaptively to fit the pressure imposed on it.

A Digital Ecosystem transcends the traditional rigorously defined collaborative environments, such as centralized (client-server) or distributed (such as peer-to-peer)

models into agent-based, loosely coupled, domain-specific and demand driven interactive communities which offer cost-effective digital services and value-creating activities that attract agents to participate and benefit from it [2].

A Digital Ecosystem is defined as a self-organizing digital infrastructure aimed at creating a digital environment for networked organizations that support the cooperation, knowledge sharing, and development of open and adaptive technologies [3] and evolutionary domain knowledge rich environments [2].

The Digital Ecosystem infrastructure is a Digital Environment which is populated by Digital Components [4]. A Digital Component is any useful idea that is expressed by a formal or natural language. This idea is digitalized and transported within the ecosystem, and can be processed by humans or by computers. A Digital Environment evolves and adapts to local conditions through the recombination and evolution of its Digital Components.

A Digital Ecosystem can be specifically developed for an anti-terrorist community, where species in the ecosystem such as various information resources and associated applications act as Anti-terrorist Digital Components that populate Anti-terrorist Digital Environment.

2. Anti-terrorist Digital Ecosystem (ATDES)

We believe that an anti-terrorist community can be supported through optimal use of the available information and linking this information to the personal machine-readable records. The information resources can be networked using a Digital Ecosystem paradigm. A network of various information resources that contain personal machine-readable information can be designed and implemented to create a Digital Ecosystem. Such an organization network may activate a virtuous circle through dynamic integration of several components that are provided by different information resources scattered around world.

We propose an Anti-terrorist Digital Ecosystem (ATDES) as Anti-terrorist Digital Environment (ATDE) populated by Anti-terrorist Digital Components (ATDC). We believe that ATDE may be prototyped on a small region but should eventually be spread globally. ATDC may include various components but the key components should be:

- ID databases that contain personal information, criminal records and related information (ATDC1)
- screening components that read personal records and match them to the available information from the ID databases (ATDC2)
- machine-readable personal records (ATDC3)

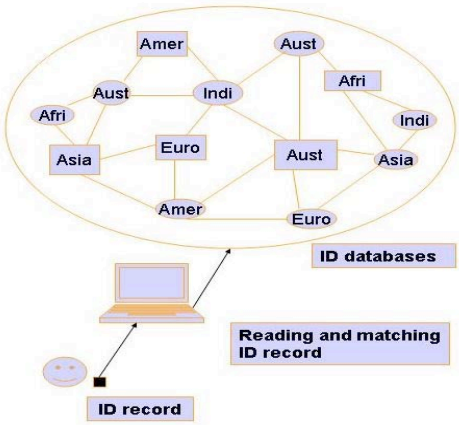

Figure 1. Anti-terrorist Digital Components (ATDC)

In Figure 1, we show the three main components of the ATDES. Different information resources from different parts of the world form a network of interrelated parts. This network is conceptually regarded as one big information resource that contains personal records of all humans inhabiting our planet. We call this component ATDC1. The second ATDES component (ATDC2) reads personal records and matches this data with personal records from the networked information resources. It is needed to place a huge number of ATDC2s in order to establish a more controlled environment. Each person carries its machine-readable personal record. This is ATDC3 that is read by ATDC2 and matched against data from ATDC1.

3. Use of Ontology within ATDES

If the available information is to be shared between various information resources, standardization of data needs to take place. Ontologies can be used for this purpose. Moreover, the use of ontologies adds semantics to the model and enables meaningful interpretation of the data.

ID Ontology can be used to keep personal information in a comprehensive format. Instantiation of the ID Ontology concepts results in specific ID Ontologies that act as personal records. Personal records from ATDC3s as well as personal records from ATDC1s are kept in the format of ID Ontology.

In Figure 2, we show ID Ontology that can be used to represent knowledge about a person. Concepts and relationships between those concepts need to be precisely defined and assembled together to uniquely describe a personal record. Assigning values and attributes to the concepts of the ID Ontology will then result in instantiated ID Ontology or personal records that uniquely describe a person.

Figure 2. Use of ID Ontology to define personal records

We propose Onto-agents as Ontology-based intelligent leading software species that have strong reasoning capabilities which can manage, coordinate and collaborate between ATDCs. Onto-agents commit to the common ID Ontology. This means they obey the agreement with respect to the semantics of the concepts and relationships defined in the ID Ontology and agree to use the shared vocabulary in a coherent and consistent manner [5]. Because Ontologies are stored as machine-readable files, Onto-agents can read personal records defined as ontology files in ATDC3s, do the matching with the available ID records defined as ontology files in networked ID databases (ATDC1s) and to take actions according to the results.

4. Digital Ecosystem and Ambient Intelligence

Ambient Intelligence (AmI) refers to digital environments that are sensitive and responsive to the presence of people [6]. This interaction between human beings and digital information technology can be established through ubiquitous computing devices such as sensors for shape, movement, scent or sound recognition [7]. AmI requires convergence of

several computing areas such as ubiquitous computing, intelligent systems, transparent technologies, context awareness and social interaction of objects in the environment [8].

The purpose of Digital Ecosystems design and use is very similar to the purpose of creation of Ambient Intelligence. Progress in AmI technologies results in development of better Digital Ecosystems, and vice versa. Those two approaches are sharing the same vision but are taking different points of view. They are highly related and interconnected but show some differences.

To explain the differences, we will take the example from nature. On a tropical island, we may have a rain forest ecosystem, a mangrove swamp ecosystem along the coast and an underwater coral reef ecosystem. Analogously, within an Intelligent Ambient, we may have three different Digital Ecosystems. The three ecosystems of a tropical island are integrated into one big Tropical Island Ecosystem and this ecosystem is further integrated with other ecosystems on our planet Earth to form a mega Earth Ecosystem. Analogously, it is most probable that two separate Digital Ecosystems may need to be integrated in order to enable effective cooperation and knowledge sharing.

Another example: the Intelligent Ambient of a train station can be established through networks of various Digital Components. Each Digital Component belongs to one of the three Digital Ecosystems. One Digital Ecosystem controls if the passengers have the correct train tickets (Ticket Control Digital Ecosystem), the second Digital Ecosystem may be designed to inform passengers about available train services (Information Digital Ecosystem) and the third Digital Ecosystem can be the one we proposed in this chapter (Anti-terrorist Digital Ecosystem). The whole ambient is intelligent and the three different ecosystems are making part of it. Machine readable personal records can be designed in such a way that it integrates data needed by each of the three different Digital Ecosystems. In this way, this personal record could be read and understood by Digital Components of each of the three different Digital Ecosystems (Ticket Control, Information and Anti-terrorist).

The integration process of Digital Ecosystems may continue and eventually, all Digital Ecosystems of various domains will form a mega Digital Ecosystem analogous to the Earth Ecosystem. However, this integration process of Digital Ecosystems is not an easy task. Having this vision of our future and being aware of the advantages of this integration as well as the problems associated with this integration process, it is best to design a Digital Ecosystem based on the latest technologies which would enable their easy integration.

Discussion and Conclusion

We proposed an Anti-terrorist Digital Ecosystem (ATDES) to protect people from terrorist attacks and innocent sufferings. This organization network activates a virtuous circle through dynamic integration of three key Anti-terrorist Digital Components (ATDCs): ATDC1 component embraces different information resources scattered around world that contain personal records, ATDC2 component reads personal records and matches this data with personal records from ATDC1, and ATDC3 component has machine-readable personal records that need to be matched against the information available in ATDC1. We

use ID Ontology to keep personal information in a comprehensive format. Instantiation of the ID Ontology concepts results in specific ID Ontologies that act as personal records.

The significance of the research lies in the unification of the advances of the Ontology technology and Ecosystem paradigm for the purpose of creating a more secure environment.

References

[1] Dini, P., Nicolai, A., 'D.B.E. - The Digital Business Ecosystem'. Retrieved: 20th of February 2006 from http://www.digital-ecosystems.org/doc/dbe_summary_cc.pdf.
[2] Chang, E., Dillon, T.S., Hussain, F.K. 2006, *Trust and Reputation for Service-Oriented Environments*, John Wiley and Sons.
[3] European Commission (a), 'Technologies for Digital ecosystems – Innovation Ecosystem Initiative'. Retrieved 20th of February 2006 from http://www.digital–ecosystems.org/
[4] European Commission (b), 'What is an European Digital Ecosystem?'. Retrieved 24th of February 2006 from http://europa.eu.int/comm/enterprise/ict/conferences/doc/p5_de2.pdf.
[5] Gruber, T. 1995, 'Towards Principles for the Design of Ontologies Used for Knowledge Sharing', International Journal of Human and Computer Studies, vol. 43, no. 5-6, pp. 907-928.
[6] Gaggioli, A. 2005, 'Optimal Experience in Ambient Intelligence', *Ambient Intelligence*, IOS Press.
[7] Alcaniz, M., Rey, B. 2005, 'New technologies for Ambient Intelligence', *Ambient Intelligence*, IOS Press.
[8] Shadbolt, N. 2003, 'Ambient Intelligence', *IEEE Intelligent Systems*, vol. 18, no. 4, pp. 2-3.