



UNIONE EUROPEA  
Fondo Sociale Europeo



## Informatica Computer Science

<b>Progetto di ricerca/ Research project</b>	<p><i>“Modelli computazionali basati su Intelligenza Artificiale del Consumatore green”</i> (codice progetto INF.1)</p> <p><i>“Artificial Intelligence-based computational models of the green consumer”</i> (project code INF.1)</p>
<b>Type</b>	Green
<b>Docente proponente/ Proposing Professor</b>	Prof. Paolo Napoletano
<b>Abstract</b>	<p><b>ITA</b></p> <p>In questi ultimi anni stiamo assistendo ad una vera e propria rivoluzione nel settore dell'economia grazie all'avvento di un nuovo paradigma chiamato “green economy” che prevede che ci sia sviluppo economico ma con riduzione dell'impatto sull'ambiente. Ricerca di nuovi materiali eco sostenibili, tecnologie di produzione dell'energia eco sostenibili, strategie per la riduzione dell'inquinamento, sono solo alcuni dei temi su cui si lavora da qualche anno per la realizzazione della green economy.</p> <p>Uno degli aspetti che al momento è ancora sottovalutato è quello relativo al comportamento del consumatore che di fatto è il principale attore della green economy. Studi recenti ci dicono infatti che il consumatore è da considerarsi un “Elusive Green Consumer” e cioè un consumatore che pur riportando una forte attitudine a comportamenti green, nella realtà non ha atteggiamenti green. Uno studio recente ha analizzato il comportamento di un gruppo di consumatori e ne deriva che: il 65% dei consumatori ha dimostrato interesse all'acquisto di brand che si dichiarano eco sostenibili ma solo il 26% dei consumatori ha effettivamente acquistato prodotti da brand eco sostenibili. Questo gap che esiste tra comportamento intenzionale e reale è un aspetto cruciale per la buona riuscita della green economy. Diversi sono gli aspetti su cui si può agire per ridurre questo gap, tra cui ad esempio: usare influenza sociale, promuovere buone abitudini, cambiare la comunicazione pubblicitaria ecc.</p> <p>Il modo con cui le aziende comunicano con i consumatori può avere un enorme impatto sull'impiego di comportamenti eco sostenibili. Le persone sono più propense ad un comportamento virtuoso quando questo comporta sensazioni positive. Ad esempio, è stato scoperto che l'uso del concetto di speranza e orgoglio è particolarmente efficace nell'influenzare positivamente il consumo sostenibile. Spesso invece le campagne pubblicitarie enfatizzano messaggi che poi risultano inquietanti per i consumatori e quindi disincentivano il consumo sostenibile.</p> <p>Lo scopo di questo progetto di dottorato è quello di sviluppare modelli computazionali basati su Intelligenza Artificiale che permettono di predire le reazioni emotive dei consumatori a stimoli audiovisivi in ambito green. Questi modelli potranno essere utilizzati per guidare le aziende nella creazione di campagne pubblicitarie più mirate ed efficaci con lo scopo di ridurre il gap del Elusive Green Consumer.</p> <p>Questo progetto prevede da prima uno studio delle reazioni del consumatore a stimoli audiovisivi e successivamente la realizzazione di un modello computazionale che possa</p>



UNIONE EUROPEA  
Fondo Sociale Europeo



imparare dai comportamenti dei consumatori e quindi possa essere in grado di sviluppare capacità predittive.

In questi studi saranno utilizzate tecniche di Deep Learning per l'analisi dei segnali audio e video ma soprattutto tecniche di Machine Learning per l'analisi non supervisionata per profilazione automatica per realizzare risposte personalizzate del modello computazionale del consumatore.

L'impatto potenziale atteso della ricerca è principalmente nel settore commerciale delle vendite dei prodotti ecosostenibili. Ci si aspetta che con i modelli computazionali che saranno sviluppati grazie a questa ricerca le campagne pubblicitarie potranno contenere elementi di suggestione positiva verso comportamenti eco sostenibili.

Sono previste milestones per la misurabilità dei risultati attesi. Ogni 6 mesi è previsto un deliverable per ognuna delle attività più salienti all'interno del progetto così come si prevede di sottoporre i prodotti della ricerca a conferenze e riviste internazionali di riferimento.

#### **ENG**

In recent years we are witnessing a real revolution in the economic sector thanks to the advent of a new paradigm called "green economy" according to which you can have economic development but with reduced impact on the environment.

The search for new eco-sustainable materials, eco-sustainable energy production technologies, strategies to reduce pollution, are just some of the issues on which researchers have been working for some years for the realization of the green economy. One of the aspects that at the moment is still underestimated is the one related to the behavior of the consumer who is in fact the main actor of the green economy. Recent studies tell us that the consumer can be considered an "Elusive Green Consumer", i.e., a consumer who, although reporting a strong attitude to a green behavior, in reality does not have green attitudes. A recent study analyzed the behavior of a group of consumers and found that: 65% of consumers showed interest in buying brands that claim to be eco-sustainable but only 26% of consumers actually bought products from eco-sustainable brands.

The aim of this PhD project is to develop computational models based on Artificial Intelligence that allow to predict the emotional reactions of consumers to audiovisual stimuli related to the green topic. These models can be used to guide companies in creating more targeted and effective advertising campaigns with the aim of reducing the Elusive Green Consumer gap.

This project considers first a study of consumer reactions to audiovisual stimuli and then the realization of a computational model that can learn from consumer behaviors and then be able to develop predictive capabilities.

In this project, Deep Learning techniques for the analysis of audio and video signals will be used, but especially Unsupervised Machine Learning techniques for automatic profiling to achieve personalized responses of the computational model of the consumer.

The expected potential impact of the research is primarily in the commercial sector of eco sustainable product sales. The computational models that will be developed through this research will permit to design advertising campaigns that contain elements of positive suggestion towards eco-sustainable behaviors.

Milestones are included for the measurability of the expected results. Every 6 months there will be a deliverable for each of the most salient activities within the project as well as the submission of research products to relevant international conferences and journals.



UNIONE EUROPEA  
Fondo Sociale Europeo



<b>Azienda/Company</b>	EMOTIVA S.r.l. (Milano)
<b>Mesi di ricerca in impresa/ Months of research in the Company</b>	6
<b>Mesi di ricerca all'estero/ Months of research abroad</b>	6
<b>Istituzione Estera/ Foreign Institution</b>	University of British Columbia



UNIONE EUROPEA  
Fondo Sociale Europeo



<b>Progetto di ricerca/ Research project</b>	<p><i>“Sistemi robotici per il controllo dell'inerbimento in colture di medio fusto”</i> (codice progetto INF.2)</p> <p><i>“Robotic systems for controlling the grassing in medium-trunked crops”</i> (project code INF.2)</p>
<b>Type</b>	Green
<b>Docente proponente/ Proposing Professor</b>	Prof. Domenico G. Sorrenti
<b>Abstract</b>	<p><b>ITA</b></p> <p>Con il termine "colture di medio fusto" si intendono colture in cui le piante di coltura sono di taglia piuttosto maggiore di quella delle più comuni malerbe. Esempi di questa taglia sono viti, olivi, agrumi. Queste piante sono comunque soggette a competizione, in modo particolare per la risorsa idrica, con le malerbe. Dal momento che l'apparato radicale di qualunque pianta ha estensione proporzionale al suo apparato fogliare, si ricorre alla limitazione dell'apparato fogliare delle malerbe allo scopo di mantenere ridotta la competizione con le piante di coltura. La pratica di completa eliminazione delle malerbe, necessaria in contesti di completa competizione con la coltura, come ad esempio in orticoltura, non è oggi ritenuta una buona pratica in quanto espone il suolo al dilavamento da parte delle acque meteoriche. Pertanto è di grande interesse lo sviluppo di sistemi autonomi per il controllo dell'inerbimento, attività che è infatti oggetto di ricerca applicata in molti centri di ricerca nel mondo (Francia, Germania, Olanda, USA, Gran Bretagna, etc.). In questo contesto si possono identificare due ambiti di sviluppo: quello relativo alla navigazione autonoma della macchina nel campo in cui ha luogo la coltura e quello relativo alla movimentazione, relativa alla macchina, del vero e proprio dispositivo di taglio delle erbe; questa movimentazione è necessaria per effettuare la lavorazione anche lungo le file della coltura, tra le piante costituenti la fila. Allo scopo di svolgere questa lavorazione sono necessarie diverse funzionalità percettive ed attuative. La macchina deve essere in grado di identificare e localizzare le piante della coltura e le malerbe, discriminando anche l'area inerbita e già lavorata da quella inerbita, ma ancora da lavorare. Questa funzionalità è di notevole complessità, considerando che durante la stagione sia le piante di coltura che le malerbe hanno uno sviluppo vegetativo che ne modifica sostanzialmente l'apparenza, che in diverse zone di coltura si hanno differenti cultivar delle piante di coltura, di differenti apparenze, e soprattutto differenti specie di malerbe, che comporta di nuovo differenti apparenze. Si deve inoltre osservare che, oltre alle variazioni di apparenza indotte dal trascorrere della stagione, anche il variare delle condizioni visive e di quelle climatiche inducono modifiche delle apparenze che dovranno essere gestite dagli algoritmi della macchina. Sarà quindi necessario sviluppare sistemi di classificazione semantica della scena circostante la macchina che siano non solo in grado di attribuire la corretta etichetta alle parti 2D / 3D di un insieme ampiamente diversificato di scene, ma anche di mantenere una corretta classificazione al variare delle apparenze. Questa funzionalità consentirà non solo il controllo locale del movimento della macchina, ma soprattutto un opportuno posizionamento del dispositivo di taglio relativamente alla macchina, coprendo anche l'area tra le piante lungo la fila di coltura. La macchina dovrà anche essere in grado di mantenere una buona stima della propria posizione (localizzazione) integrando misure ottenute da sistemi GNSS, quando queste misure siano disponibili ed affidabili, con le osservazioni di parti della scena la cui posizione sia nota (piante di coltura, pali, altri alberi, edifici, etc.). Anche questa funzionalità di localizzazione dovrà risultare compatibile con l'evolversi dell'apparenza delle parti della scena nel corso della stagione ed al variare delle condizioni visive e climatiche. Questa funzionalità di localizzazione implica la disponibilità</p>



UNIONE EUROPEA  
Fondo Sociale Europeo



di una mappa e, per la assenza di mappe dettagliate delle colture (a differenza da quanto accade in ambito di guida su strada urbana, dove esiste un mercato delle mappe, con diversi attori), servirà che la macchina sia autonomamente in grado di effettuare la costruzione di una mappa della scena, che risulti usabile al variare dell'apparenza delle parti di scena. Anche questo aspetto non è presente nello stato dell'arte corrente.

**ENG**

With the term "medium-trunked crops" we here mean crops where the crop plants are of a quite larger size w.r.t. the most common weeds. Examples of such size are vines, olives, citruses, etc. Such plants are subject to competition, in particular for the water, with the weeds. Given that the root apparatus of any plant has an extent proportional to the leaf apparatus, it is usual to limit the leaf apparatus of the weeds, in order to keep limited the competition with the crop plants. The practice of complete elimination of the weeds, still required in cases of full competition with the crop, like in horticulture, is not considered to be a good practice as of today for medium-trunked crops, because it exposes the soil to rainwater runoff. It is therefore of great interest to develop autonomous systems for controlling the grassing, which is actually an ongoing research activity in many research centres in the world (France, Germany, Netherlands, USA, Great Britain, etc.). In this context, two areas of work can be identified: the autonomous navigation of the machine in the crop field, and the movement, relative to the machine, of the grass cutting device; this movement is required to carry out the process also along the crop rows, in between the crop plants making up the row. In order to perform such processing a few functionalities are necessary both in perception and actuation. The machine has to be able to identify and localize the crop plants and the weeds, discriminating also the grass already processed from the grass still to be processed. This classification functionality is quite a difficult one, considering that during the crop season both the crop plants and the weeds undergo a vegetative growth that significantly alters their appearance, considering that in different areas of the world / country different cultivars of the crop are in use, whose appearance also differs, considering also that different weeds live in the different areas, again presenting different appearances. Moreover, it has to be noted that, besides the changes in appearance due to the moment in the season, also the changes in the day and in the weather conditions heavily affect the appearances. All such changes should be smoothly handled by the machine algorithms. It will be therefore necessary to develop a semantic classification of the scene about the machine, capable to properly classify the 2D / 3D parts of a largely diversified set of scenes, but also to provide a correct classification with the changing appearances. This functionality will allow not only the local navigation of the machine, but it will be mainly used to control the positioning of the cutting device, to process also the area along the crop row. The machine will also need to keep small the uncertainty on its pose estimate (localization) integrating measures obtained from GNSS systems, when such measures are available and reliable, with measures of parts of the scene whose position is known (crop plants, poles, other trees, buildings, etc.). Also the localization functionality has to cope with the evolution of the appearance of parts of the scene during the crop season, daylight, and weather conditions. The localization functionality implies the availability of a map and, because of the absence of detailed maps of the crop field (differently from what happens in road autonomous driving, where there is a market of maps, with different players), an autonomous mapbuilding functionality is needed onboard the machine, which also is required to adapt to the change of appearance of scene parts. Also this last aspect is not available in the state of the art

**Azienda/Company**

Info Solution Spa (Vimodrone)



UNIONE EUROPEA  
Fondo Sociale Europeo



<b>Mesi di ricerca in impresa/ Months of research in the Company</b>	6
<b>Mesi di ricerca all'estero/ Months of research abroad</b>	6
<b>Istituzione Estera/ Foreign Institution</b>	Albert-Ludwigs-Universität Freiburg, Germany oppure Universidad de Alcalá - Alcalá de Henares, Spain



<b>Progetto di ricerca/ Research project</b>	<p><i>“Framework dinamico per la gestione delle minacce alla sicurezza informatica”</i> (codice progetto INF.3)</p> <p><i>“Dynamic cybersecurity threat management framework”</i> (project code INF.3)</p>
<b>Type</b>	Innovative
<b>Docente proponente/ Proposing Professor</b>	<p>Prof. Fabio Sartori</p> <p>Prof. Marco Savi</p>
<b>Abstract</b>	<p><b>ITA</b></p> <p>Questo progetto di dottorato mira a definire e prototipare un framework innovativo per la gestione delle nuove minacce emergenti nello scenario della cybersecurity. L'approccio tradizionale alla sicurezza delle informazioni si basa su una combinazione solida ma statica di misure preventive (sicurezza della rete, controlli di accesso, hardening del sistema operativo), con opzioni reattive spesso limitate dalla necessità dell'intervento umano. Questo approccio è messo in discussione dal costante sviluppo di nuovi modelli e strategie di attacco e dall'innovazione tecnologica che modifica la natura stessa delle risorse da proteggere (infrastrutture virtualizzate e sistemi cyber-fisici). I nuovi requisiti più importanti da considerare in tale scenario possono essere sintetizzati come segue:</p> <ul style="list-style-type: none"> <li>• la criminalità informatica è diventata un'industria, nel dark web vi è un'ampia disponibilità commerciale di malware e informazioni/credenziali rubate;</li> <li>• (di conseguenza) il numero di potenziali aggressori è diventato enorme, e molti di loro sono mossi da motivazioni non razionali (tecnicamente, da funzioni di reward sconosciute);</li> <li>• le infrastrutture critiche e, più in generale, i sistemi cyber-fisici presentano superfici di attacco inusuali e spesso dispongono di risorse limitate (es. computazionali) da dedicare ad attività difensive; • in tali sistemi, l'obiettivo proprio della cybersecurity dovrebbe essere più correttamente definito in termini di resilienza (capacità di svolgere una funzione prevista nonostante un attacco) piuttosto che di sicurezza assoluta (nessun accesso a risorse protette).</li> </ul> <p>Da queste considerazioni derivano le caratteristiche del framework sviluppato nel progetto. Dovrà essere dinamico per natura, con enfasi su due aspetti:</p> <ul style="list-style-type: none"> <li>• la possibilità di adattarsi a schemi di attacco impreveduti (eventualmente effettuati da aggressori con reward function sconosciute);</li> <li>• la capacità di graduare la risposta secondo una funzione di costo che tenga conto sia delle possibili limitazioni delle risorse disponibili sia della necessità di limitare l'impatto sugli utenti finali. Lo sviluppo del framework richiede sforzi di ricerca in tre aree specifiche, ovvero rilevamento degli attacchi, strategia di difesa e metodi di risposta flessibili.</li> </ul> <p>La tecnica di rilevamento degli attacchi integrerà sia l'identificazione di schemi di attacco noti sia il rilevamento di anomalie, ovvero l'allontanamento delle azioni di alcuni utenti dai normali schemi di comportamento. Il primo problema può essere risolto con tecniche note (spesso chiamate tecniche signature-based, come l'attack tree modeling) sebbene le loro estensioni necessarie per affrontare ambienti che cambiano nel tempo (per l'utilizzo, ad esempio, di tecniche di Moving Target Defense) non siano completamente sviluppate. Il secondo problema (trovare tecniche efficaci di anomaly detection) vede soluzioni meno consolidate: l'uso di tecniche di Machine</p>



Learning per modellare i comportamenti "normali" è probabilmente il percorso più naturale da seguire. Inoltre un'integrazione computazionalmente efficace dei due meccanismi è un problema di ricerca aperto, con possibili contributi provenienti dall'area del Complex Event Processing. Per quanto riguarda la determinazione della migliore strategia di difesa, si ritiene che l'approccio più appropriato debba basarsi sulla teoria dei giochi stocastici con informazioni imperfette. Negli ultimi anni sono stati pubblicati diversi studi su questo argomento, ma nessun modello di gioco specifico è emerso come la scelta migliore.

L'utilità della modellizzazione della teoria dei giochi è fortemente correlata alla disponibilità di un ricco insieme di strumenti di difesa flessibili, il cui costo ed efficacia possono essere catturati da una opportuna funzione di utilità. Strumenti di questo genere esistono e alcuni di essi sono stati oggetto di un'intensa attività di ricerca negli ultimi anni: l'esempio più eclatante è l'MTD (Moving Target Defense). Altri meccanismi di difesa da considerare sono la dissimulazione con honeypot, la chiusura dei servizi o, all'estremo opposto, anche il non fare nulla (se il possibile danno è piccolo).

Questi sono i tre filoni di ricerca seguiti nel progetto, che inizierà con un'ampia analisi della letteratura, quindi si concentrerà sulla definizione degli algoritmi chiave, occupandosi in particolare dell'implementazione efficiente di tecniche integrate di rilevamento degli attacchi, e infine produrrà un dimostratore, adatto all'ambiente della società Lottomatica.

Lottomatica fa parte del gruppo IGT, il più grande fornitore mondiale di servizi di gioco e scommesse on-line. Il gran numero di transazioni servite, il significativo valore economico coinvolto e i severi requisiti in tempo reale rendono questo ambiente particolarmente impegnativo per la sicurezza informatica. Lottomatica metterà a disposizione i dati relativi al normale comportamento di diverse tipologie di utenti dei propri sistemi (utenti finali, altri fornitori di servizi, amministratori) e aiuterà nella creazione di un ambiente di test in cui il dimostratore agirà in shadow mode, parallelamente ai tool commerciali impiegati per proteggere i sistemi in esercizio.

### ENG

This doctoral project aims at defining and prototyping an innovative framework for managing the emerging threats in the cybersecurity scenario. The traditional approach to information security is based on a solid but static arrangement of preventive measures (network security, access controls, OS hardening), with reactive options often limited by the need of human intervention. This approach is challenged by the constant development of new attack models and strategies, and by the technological innovation changing the nature of the resources to be protected (virtualized infrastructures and cyber-physical systems). The most important new requirements to be considered in such a scenario may be synthesized as follows:

- cybercrime has become an industry, with the dark web featuring a large commercial availability of malware and stolen personal information/credentials;
- (as a consequence) the number of potential attackers has become huge, and many of them are moved by non-rational motivations (technically, by unknown reward functions);
- the critical infrastructures and, more generally, the cyber-physical systems exhibit unusual attack surfaces and often have limited resources (e.g. computational) to devote to defensive activities;
- in such systems, the proper objective of cybersecurity should be more correctly stated in terms of resiliency (capacity to carry out an intended function in spite of an attack) as opposed to absolute security (no access to secured assets).

The characteristics of the framework developed in the project derive from these considerations. It shall be dynamic in essence, emphasizing:





	<ul style="list-style-type: none"> <li>• the possibility to adapt to unexpected attack patterns (possibly carried out by attackers with unknown reward functions);</li> <li>• the capacity to grade the response according to a cost function which will take in consideration both the possible limitations in the available resources and the need to limit the impact on end users. The framework development asks for research efforts in three specific areas, that are attack detection, defense strategy and flexible response methods.</li> </ul> <p>The attack detection technique will integrate both the identification of known attack patterns and the detection of anomalies, that is the departure of the actions of some users from the normal behavior patterns. The former problem can be solved by known techniques (often called signature-based techniques, such as attack tree modeling) although their extensions necessary to deal with environments changing in time (due for instance to Moving Target Defense techniques) are not completely developed. The latter problem (finding effective anomaly-based techniques) is less understood: the use of Machine Learning techniques to model “normal behaviors” is probably the most natural pathway to follow. Moreover the computationally effective integration of the two mechanisms is an open research problem, with possible contributions coming from the Complex Event Processing area.</p> <p>For what concerns the determination of the best defender’s strategy, it is believed that the most appropriate approach should be based on stochastic game theory with imperfect information. Several studies on this topic have been published in recent years, but no specific game model has emerged as the best choice. The usefulness of game-theoretic modelling is strongly related to the availability of a rich set of flexible defense tools, whose cost and effectiveness can be captured by a suitable utility function. As a matter of fact, such tools do exist and some of them have been subject to intensive research activity in recent years – the most prominent example being MTD (Moving Target Defense). Other defense mechanisms to be considered are deception/honeypots, shutting down services or, at the other extreme, even do-nothing (if the possible damage is small).</p> <p>These three research streams will be undertaken in the project, which will begin with an extensive literature analysis, then concentrate on the key algorithms definition, especially dealing with the effective implementation of the integrated attack detection techniques, and finally produce a demonstrator, suited to the environment of the Lottomatica company.</p> <p>Lottomatica is part of the IGT group, the largest worldwide provider of on-line gaming and betting services. The large number of transactions served, the significant economic value involved and the stringent real-time requirements make this environment particularly challenging for cybersecurity.</p> <p>Lottomatica will make available the data regarding the normal behavior of several kinds of users of its systems (end users, other service providers, administrators) and help in setting up a testing environment where the demonstrator would act in shadow mode, in parallel to the commercial tools employed for protecting the systems in operation.</p>
<b>Azienda/Company</b>	SED MULTITEL S.r.l.
<b>Mesi di ricerca in impresa/ Months of research in the Company</b>	6



UNIONE EUROPEA  
Fondo Sociale Europeo



<b>Mesi di ricerca all'estero/ Months of research abroad</b>	6
<b>Istituzione Estera/ Foreign Institution</b>	University of Alcalà de Henares