OPPORTUNITIES AND SECURITY THREATS POSED BY NEW TECHNOLOGIES

Geert De Cubber
Unmanned Vehicle Centre
Department Mechanics
Royal Military Academy
B 1000, Brussels,
Belgium
E-mail: geert.de.cubber@rma.ac.be

KEYWORDS
Augmented reality, unmanned aerial systems, drones, unmanned maritime systems, unmanned ground systems, societal acceptance.

ABSTRACT

The technological evolution is introducing in a fast pace new technologies in our everyday lives. As always, these new technologies can be applied for good causes and thereby give us the opportunity to do many interesting new things. Think for example about drones transporting blood samples between hospitals. However, like always, new technologies can also be applied for bad causes. Think for example about the same drones, but this time transporting bomb parcels instead of blood.

In this paper, we will focus on a number of novel technologies and discuss how security actors are currently doing their best to maximize the "good" use of these tools, while minimizing the "bad" use. We will focus on research actions taken by Belgian Royal Military Academy in the domains of:

- Augmented reality, and showcase how this technology can be used to improve surveillance operations.
- Unmanned Aerial Systems (Drones), and showcase how the potential security threats posed by these systems can be mitigated by novel drone detection systems.
- Unmanned Maritime Systems, and showcase how this technology can be used to increase the safety at sea.
- Unmanned Ground Systems, and more specifically the autonomous cars, showcasing how to prevent potential cyber-attacks on these future transportation tools.

INTRODUCTION

Advances in micro-electronics and robotics are changing our society. New technologies like unmanned vehicles and augmented reality are being introduced very rapidly. Like all technologies, these can be used for good or for bad purposes and it is up to the public society to drive the societal acceptance of these technologies and up to the policy makers to create a legal framework that allows for a fair and responsible use of these new technologies. However, the fast pace in which these new technologies are introduced makes it very hard for the general public to evaluate the advantages and disadvantages of these technologies and also makes it very difficult for policy makers to adapt the legal framework to the latest evolutions. This creates a tension field between technology enthusiasts – who want to introduce these new technologies as soon as possible and sometimes neglect the societal, safety and security implications this may have – and technology conservatives – who tend to want to over-regulate novel technologies, thereby impeding their chances to mature.

Indeed, each new technology provides new opportunities, but also new threats, which then leads to other new policies or technologies that have to be developed to mitigate these threats. This paper confronts this problem by developing 4 use cases where each time a different new technology application is showcased (augmented reality, unmanned aerial vehicles, unmanned maritime vehicles and unmanned ground vehicles) and where a different aspect of the opportunities-threats-mitigation – spectrum is focused upon.

The use cases developed in this paper are based on different research actions performed in the Belgian Royal Military Academy and therefore have as application domain the broad security sector.

The objective of this paper is not to scare the reader about the security threats tied to new technologies, but to provide a balanced discussion for each of the technology areas, in order to provide the reader an insight in the advantages of each of the discussed technologies, the associated security threats that may hamper societal acceptance of the technology and the mitigation actions that are currently being under development in order to provide answers to these security threats.

AUGMENTED REALITY: HOW TO USE THIS TECHNOLOGY TO IMPROVE SURVEILLANCE OPERATIONS?

Opportunities

Security and surveillance agents have to correctly interpret any suspicious acts or anomalies and act swiftly upon confirmed threats in a coordinated manner. This is a tremendously difficult task, as these agents:

- are confronted with an overload of information, certainly as they are often surveilling densely populated areas
- have to decide upon a coordinated action plan in a minimum of time, as terrorist attacks have proven to be carried out very quickly
- have to proceed with extreme caution when entering into action, as they are working in theatres with many civilian bystanders.

Technologic aids to assist security and surveillance agents in each of these phases of the sense-plan-act decision chain have been developed in labs, but - apart from the wireless communication area – there have been few technologies that have been really successful in showing an operational advantage on the field for these kinds of applications. This is mainly due to the extremely short reaction time required, which voids the use of classical management and coordination tools (as even using tablets would distract the surveilling agent from the threat/target). However, with the advent of wearable augmented reality technology becoming more mature, portable and accessible, this situation is changing now. Indeed, augmented reality provides a paradigm for superimposing in real-time important information to the view-field of the security and surveillance agents (Azuma 1997), thereby enhancing the current perception of the reality by superimposing computer-generated sensory data, such as graphics, video, GPS data, …. A crucial aspect is of course the human-system integration and the selection of the 'augmented' information to be presented.

In order to capitalize on these potential benefits augmented reality technology can bring to security professionals, the Belgian Royal Higher Institute for Defence has decided to fund a research action that aims to develop these technologies. The envisaged solution of this research project has the following objectives:

- Enhance the security agent sensing capabilities by showing data from available mounted and dismounted sensors (video, thermal, potentially also from drones) in order to allow the agent to see around occlusions (e.g. across a corner or inside a building), as depicted on Figure 1.
- Enhance the security agent's planning capabilities by providing a continuous location information on teammates and a continuous communication channel with these teammates, including routing support in order to get to intervention locations quicker, as depicted on Figure 1.
- Preserve the security agent's existing intervention capabilities by ensuring a well-thought human-system integration that respects the security agent's requirements towards system portability and unobtrusiveness.
- Enhances the security agent's intervention capabilities by providing an augmented reality training program, wherefore augmented is particularly suited, as trainees see each other through their natural vision, as opposed to virtual reality.

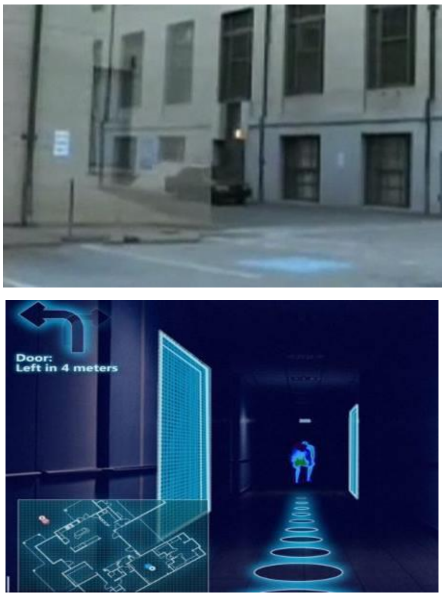

Figure 1: Concept sketch of see-through-wall user interface and localization & planning user interface

Threats

The main threat to society related to augmented reality lies in the privacy and data protection issues related to the use of the technology. Indeed, in China, the government has already begun (EDPS 2019) to roll out augmented reality glasses with automated face detection that enable police officers to automatically cross-reference faces against a national database, and single out suspects and criminals. One of the controversial aspects of this augmented reality system is that whenever the police officers are confronted with an individual, they now immediately get informed about a whole series of sensitive personal data, including the divisive social behaviour score. This means that there is a serious risk of bias by the police in the approach of individuals, which would be detrimental to the fundamental rights of each citizen. This example shows that, whereas this type of augmented reality application could be used for good uses, the risks are high. Human rights activists and data protection services have already warned (EDPS 2019) that using augmented reality technology in combination with large centralized databases containing sensitive personal information is a serious potential threat to the freedom of thought. Moreover, the data protection of sensitive personal information streamed from and to the augmented reality device (which is small and mobile and can thus be easily stolen) cannot be 100% guaranteed.

Threat mitigation

In response to the ethical concerns related to technology discussed above, it was decided not to include aspects of face mapping to a central database into the research study of the Belgian Royal Higher Institute for Defence. While this is potentially a high-value application of augmented reality technology, the privacy impact is considered too high and as long as this issue is not tackled and as long as the data protection cannot be guaranteed, it would be dangerous to field such a technology at wide scale.

UNMANNED AERIAL SYSTEMS (DRONES): HOW TO DETECT DRONES WITH MALICIOUS INTENT?

Opportunities

Recent advances in technology have rendered unmanned aerial systems (commonly referred to as drones) affordable, accessible and easily controllable by novice users. Together with the liberalization of the legal framework (which is still on-going), this has sparked the uptake of the technology for recreational use, but also for commercial use. Multiple good causes can also be referenced where drones are used for the benefit of the society, such as search and rescue (De Cubber et al. 2013) or humanitarian demining (Yvinec et al. 2012).

Threats

The enormous potential of unmanned aerial systems has unfortunately also already sparked the interest of malevolent individuals who use the technology for criminal or terrorist use (Buric and De Cubber 2017), e.g. for terrorist attacks, activism, drugs and human trafficking, privacy invasion, etc. The main problem with present-day drones is that they have become so small and agile that they virtually impossible to detect by classical detection methodologies for aerial threats (which is typically a RADAR installation). Furthermore, as the drones become more and more capable, it becomes possible to carry potentially hazardous payloads and to perform sophisticated attack operations, even with very cheap and commonly available drone platforms.

Threat mitigation

In the longer future, it will likely become mandatory for commercial drones to be registered and the systems will likely automatically register themselves (e.g. via the 5G network) with a sort of unmanned traffic management system (Lundberg et al. 2018) before taking off. This approach would resolve suite a lot of issues with recreational users unknowingly performing illegal flights.

However, an unmanned traffic management system will not solve the problem of criminals wilfully using drone technology for bad causes. Indeed, drone development kits and open-source autopilots are commonly available. As a result, it will always be possible for individuals to develop their own drone systems and by doing so bypass the mandatory registration (which is e.g. much harder when it comes to cars and regular aeroplanes). For this reason, it is required to develop a drone detection capacity.

Several detection modalities are being researched to tackle this problem: RADAR (Li and Ling 2017), LIDAR (de Haag et al. 2016), Acoustic Sensing (Mezei and Molnár 2016), Radio Sensing (Sit et al. 2016), thermal and visual sensing. As no individual sensing modality attains satisfying levels of accuracy, a combination of approaches is often used.

The most common drone detection systems are based on the RADAR sensing technology. These drone detection systems are in fact evolutions of former bird detection RADAR installations on airports that were specifically tweaked to be able to single out drones instead of birds. However, the problem with these RADAR-based drone detection systems is that they are generally quite expensive, whereas the detection range stays relatively low. As a result, the economic viability of deploying these RADAR-based drone detectors on a wide scale for protecting a large area is at this moment still questionable.

The European Commission noted this capability gap and decided in 2016 to fund the H2020-SafeShore project (De Cubber et al. 2017). The SafeShore core solution for detecting small targets that are flying in low attitude is to use a 3D LIDAR that scans the sky and creates above the protected area a virtual dome shield. In order to improve the detection, SafeShore integrates the 3D LIDAR with passive acoustic sensors, passive radio detection and video analytics. Compared to the more traditional RADAR-based detectors, all those technologies can be considered as low cost and "green" technologies, as the sensors do not emit in the radio-spectrum. The SafeShore detection system, shown on Figure 2, was implemented as a proof setup for maritime border security, detecting maritime border infringements (e.g. by human and drug traffickants, but also by terrorists) coming from over sea. The SafeShore system was validated (Doroftei and De Cubber 2018) in 2018 using three validation campaigns in the North Sea, the Mediterranean Sea and the Black Sea, showcasing that the combination of orthogonal technologies used (LIDAR, passive radio, acoustic and video analytics) show a true potential for complementing the traditional RADAR-based solutions. However, like the RADAR-based solutions, also the SafeShore system currently still has to solve many issues related to limited range and relatively high cost (be it lower than RADAR), posing bottlenecks for wide-range adoption.

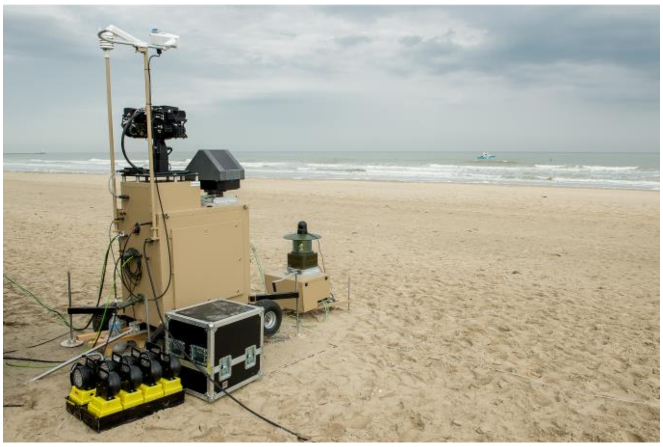

Figure 2: SafeShore drone detection system installed on the beach in Belgium during the SafeShore North Sea trial
Picture by Daniel Orban

Obviously, detection is only one first step in the complete counter-drone response chain. Effective classification, identification and even neutralization means are also required in order to provide a holistic response. In each of these areas, research is under way in order to provide responses. The main difficulty here lies in developing solutions that are also applicable in dense urban areas where there are many other legitimate drone users of the airspace or innocent bystanders that shouldn't be disturbed, rendering solutions like non-directive radio or GPS jamming & spoofing and kinetic approaches impossible.

UNMANNED MARITIME SYSTEMS: HOW TO USE THIS TECHNOLOGY TO INCREASE THE SAFETY AT SEA?

Opportunities

Unmanned maritime platforms are now becoming more and more a mature technology. They are increasingly used by law enforcement agencies worldwide and are forecast to grow quickly over the next decade. In the US, unmanned maritime platforms were identified as a key enabler for maritime security and electronic surveillance. In Europe, the European Defence Agency has explored their use for military applications and identified long term deployment, mission planning and interoperability as the key issues to be tackled for their routine use for maritime surveillance operations.

The aim of maritime surveillance is to understand, prevent (where applicable) and manage the actions and events that can have an impact on Maritime Safety and Security, search and rescue, accident and disaster response, fisheries control, marine pollution, customs, border control, general law enforcement and defence, as well as on the economic interests. To date, this has been undertaken using satellites (remote sensing), aircrafts and manned ships equipped with a variety of sensors, from radars to thermal imagery. Unmanned Maritime Systems have the potential to provide significant benefits to bodies involved in maritime surveillance.

First, they can provide round the clock operations and remove the human from the operating scene. Second, their low-cost compared to currently used manned assets makes them suitable as a force multiplier to enhance and, in the longer term, replace existing maritime platforms. Finally, with suitable embedded intelligence, they can be used collaboratively for complex surveillance tasks on a large scale.

New developments in solar and wind powered systems pave the way for the more permanent deployment of unmanned maritime systems and makes them ideal as host platforms for other unmanned assets such as Unmanned Underwater Systems and Unmanned Aerial Systems with more limited autonomy.

Another reason that unmanned maritime platforms are so ideally suited for maritime surveillance is that they typically have a low radar and heat profile and can approach and qualify potential illegal activities safely and effectively while potentially staying undetected until other assets can be deployed.

They can also be used to deploy complementary sensors, either mobile such as Unmanned Aerial Systems, Blimps and Unmanned Underwater Systems to enable a very wide variety of sensors to work collaboratively. Uniquely, they can detect maritime targets with low profiles such as rubber boats and submersible or semi-submersible vehicles and can thus be deployed in various scenarios, e.g. the fight against piracy, smuggling and illegal fishing or used as a screen against hostile operations or for safeguarding shipping and sea lanes.

Threats

As unmanned maritime systems are mostly employed at sea, they come less into contact with the general public and there are less security and societal acceptance issues to be solved that may hamper a wide-scale adoption of the technology, compared to unmanned ground and aerial systems. This is also the reason why unmanned maritime systems are much more mature in terms of autonomy features compared to their aerial and ground-based siblings, even though this may be much less visible to the general public.

This also means that more and more of these vehicles are being deployed in the field, each with their own characteristics and specifications. This variety of systems is now starting to pose interoperability problems when deploying multiple of these unmanned maritime systems together for operations, as there is to date no unified command structure for these unmanned assets and there are also no standardized data interchange platforms that allow for an easy transfer of sensory information from one platform to another. The result is that commanders of unmanned maritime systems have to work in most circumstances with custom-built solutions that may be good in performing one task well, but that encompass little flexibility and modularity towards upgrading the task description for future needs or towards interoperability with other deployed assets.

Threat mitigation

Responding to the increasing problems related to interoperability in the domain of unmanned maritime systems, the Belgian Royal Higher Institute for Defence has decided to fund a research action that aims to develop a heterogeneous interoperability and collaboration framework which is seamlessly interoperable with the existing and future C4I and GIS infrastructure. The interoperability concept consists of a highly modular system of carrier platforms and payloads like the systems depicted on Figure 3, enabling straightforward switching of payloads from one system to another.

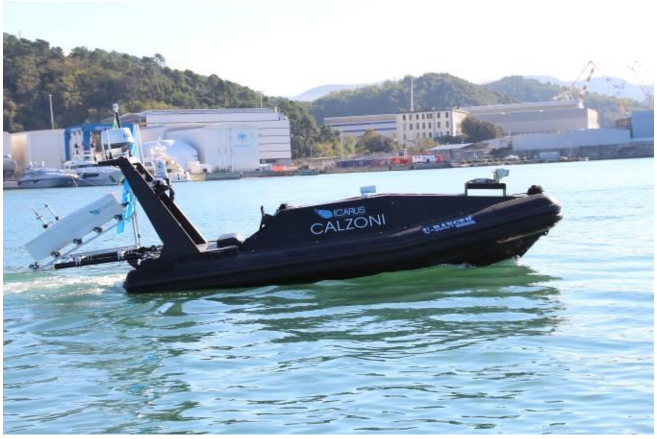

Figure 3: Two Unmanned Maritime Systems (fast mothership carrying a rescue capsule) for search and rescue operations (De Cubber et al. 2013)

UNMANNED GROUND SYSTEMS: HOW TO PREVENT CYBER-ATTACKS ON OUR FUTURE AUTOMATED CARS?

Opportunities

The scientific advances made in the field of robotics have led to an increase in the number of unmanned ground vehicles used. Two main application domains are currently using unmanned ground vehicles in large numbers. On one hand there is the military, where they are used as Explosive Ordnance Disposal robots, search and rescue robots or demining robots. On the other hand, there is the application field of distribution and warehouse automation, where whole large-scale warehouses see a transformation from traditional human-led pick & place operations towards automated services provided by robots.

In this section, we will however develop and discuss another type of unmanned ground vehicle: the self-driving cars. When discussing self-driving cars, it is important to distinguish the 5 levels of automation for these vehicles, going from 0 (no automation) to 5 (fully autonomous in all areas under all roadway and environmental conditions). Currently, some manufacturers provide autopilot systems that are capable of reaching level 2 (partial automation, e.g. on motorways) and in research level 4 can even be attained, where the system only needs to fall back to a human in exceptional cases. Even though there are today no truly fully autonomous self-driving cars on the market (which would mean level 5 automation), the market potential for these types of vehicles is huge and so is the potential disruption they can cause to society. Therefore, several (mostly all) car companies and many technological giants like Google are currently developing self-driving cars, as shown on Figure 4.

Figure 4: Waymo self-driving minivan during testing (Picture by Dllu [CC BY-SA 4.0])

The potential benefits to society of self-driving cars are huge. In the first place, there is the safety argument. Indeed, in many developed countries, road accidents have become the most prominent cause of death for young adults (20 to 40 years) and self-driving cars hold the promise to bring down that number of deaths significantly. Even though autonomous driving cars can become safer than humans driving cars, this promise shouldn’t be taken for granted, it still needs to be proven, and it should also be very clear to everyone that bringing down the accident rate to zero is not realistic.

Furthermore, self-driving cars bring with them the promise of mobility as a service, where car ownership is no longer necessary, but people can hail self-driving taxis whenever they need them. This would also void the need for garages and parking spaces that take up enormous amounts of public space in our cities (and homes), making room for more a useful application of that space.

Threats

The potential threats posed by self-driving cars are multiple. First, these vehicles rely on multiple sensors in order to avoid obstacles and interpret the situation on the road. The most common sensing technologies include RADAR, LIDAR, and cameras. The issue is that each of these sensors have their specific failure modes, i.e. situations where they totally misinterpret the situation, which could lead to deadly accidents.

Concerning RADAR systems, researchers have shown a technique (Yan et al. 2016) to fool the system into perceiving an object where none existed, leading to dangerous evasive manoeuvres. Concerning the LIDAR, researchers have demonstrated (Shin et al. 2017) two kinds of attacks: a spoofing attack, and a saturation attack. While both LIDAR and RADAR hacks do require some specialist equipment, cameras can be fooled much easier, by putting stickers on street signs. Researchers (Eykholt et al. 2018) analysed the machine learning algorithms used by the cars and applied a number of different attacks to manipulate signs in order to trick machine learning models into misreading them, applying some small stickers to trick the vision system an autonomous car would use into reading a stop sign as a 45-mile-per-hour sign, which could lead to accidents.

A whole different threat is related to data and privacy protection. Indeed, the improvement in the autonomy of self-driving cars depends on the continuous feedback and improvement of the machine learning algorithms that are fed data from the car’s sensors. This entails that the self-driving cars constantly send – potentially sensitive – data acquired by their sensors to the manufacturers, which is a data protection risk.

Threat mitigation

There is only one possible solution to the problem with the individual failure modes of the different sensors: redundancy. Indeed, like in the aircraft industry, it will probably become mandatory for future self-driving cars to use different, redundant and independent sensing modalities in order to be “roadworthy”. Using novel sensors (De Cubber et al. 2011), multi-modal sensor combinations (De Cubber and Doroftei 2011), and intelligent data fusion it is possible to recover from failures from individual sensors and build up a robust environmental picture in all circumstances.

It needs to be noted that this demand for redundancy comes at a cost: it means that all self-driving cars will have to be equipped with multiple expensive sensors and probably also with multiple expensive processing stations, which means that the cost for a self-driving car will probably be high (which may become less of a concern as car ownership will probably no longer be required).

CONCLUSIONS

Within this paper, we have discussed four novel technologies (augmented reality, unmanned aerial vehicles, unmanned maritime systems, self-driving cars) and how they can impact our society: what opportunities lay ahead of us, but also what threats these new technologies pose to us and what can be done to mitigate these threats. In all of these four areas, the Belgian Royal Military Academy is active in providing solutions to promote and increase the "good" use of the technology and to prevent the "bad" use. By doing so, we hope to promote the societal acceptance of these technologies and to contribute to a safer and more secure world.

REFERENCES

Azuma, R.T. 1997. "A Survey of Augmented Reality". In *Presence: Teleoperators and Virtual Environments* 6, No. 4 (August), 355-385

Buric, M. and De Cubber, G. "Counter Remotely Piloted Aircraft Systems", *MTA Review*, Vol. 27, No. 1, Military Technical Academy Publishing House, June 2017

De Cubber, G.; Doroftei, D.; Sahli, H. and Baudoin, Y. 2011. "Outdoor Terrain Traversability Analysis for Robot Navigation using a Time-Of-Flight Camera," *in Proc. RGB-D Workshop on 3D Perception in Robotics*, Vasteras, Sweden

De Cubber, G. and Doroftei, D. 2011. "Multimodal terrain analysis for an all-terrain crisis Management Robot," in *Proc. IARP HUDEM*, Sibenik, Croatia.

De Cubber, G.; Doroftei, D.; Serrano, D.; Chintamani, K.; Sabino, R.; Ourevitch, S. 2013. "The EU-ICARUS project: developing assistive robotic tools for search and rescue operations". *IEEE international symposium on safety, security, and rescue robotics (SSRR).* (October)

De Cubber, G.; Shalom, R.; Coluccia, A.; Borcan, O.; Chamrád, R.; Radulescu, T.; Izquierdo, E.; Gagov, Z. 2017. "The SafeShore system for the detection of threat agents in a maritime border environment", *IARP Workshop on Risky Interventions and Environmental Surveillance*, Les Bons Villers, Belgium, (May)

Doroftei, D.; De Cubber, G. 2018. "Qualitative and quantitative validation of drone detection systems", *International Symposium on Measurement and Control in Robotics* ISMCR2018, Mons, Belgium (September).

de Haag, M. U.; Bartone, C. G.; and M. S. Braasch, 2016. "Flight-test evaluation of small form-factor LiDAR and radar sensors for sUAS detect-and-avoid applications," *IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, Sacramento, CA, pp. 1-11

EDPS. 2019. "Technology report No 1 - Smart glasses and data protection", European Data Protection Supervisor, Brussels, January.

Eykholt, K.; Evtimov, I.; Fernandes, E.; Li, B.; Rahmati, A.; Xiao, C.; Prakash, A.; Kohno, T.; Song, D. 2018. "Robust Physical-World Attacks on Deep Learning Models". In *IEEE Computer Vision and Pattern Recognition*.

Li, C. J. and Ling, H. 2017. "An Investigation on the Radar Signatures of Small Consumer Drones," in *IEEE Antennas and Wireless Propagation Letters*, vol. 16, no. , pp. 649-652

Lundberg, J.; Palmerius, K.L.; Josefsson, B. 2018. "Urban Air Traffic Management (UTM) Implementation In Cities – Sampled Side-Effects" *IEEE/AIAA 37th Digital Avionics Systems Conference (DASC).*

Mezei, J. and Molnár, A. 2016. "Drone sound detection by correlation," *IEEE 11th International Symposium on Applied Computational Intelligence and Informatics (SACI)*, Timisoara, pp. 509-518

Shin, H.; Kim, D.; Kwon, Y. and Kim, Y. 2017. "Illusion and Dazzle: Adversarial Optical Channel Exploits against Lidars for Automotive Applications". In *International Conference on Cryptographic Hardware and Embedded Systems (CHES).* pp 445-467

Sit, Y. L. ; Nuss, B.; Basak, S.; Orzol, M.; Wiesbeck, W. and Zwick, T. 2016. "Real-time 2D+velocity localization measurement of a simultaneous-transmit OFDM MIMO Radar using Software Defined Radios," *European Radar Conference (EuRAD)*, London, 2016, pp. 21-24

Yan, C.; Xu, W.; Liu, J. 2016. Can You Trust Autonomous Vehicles: Contactless Attacks against Sensors of Self-Driving Vehicles. In *DEFCON Conference*

Yvinec, Y.; Baudoin, Y.; De Cubber, G.; Armada, M.; Marques, L.; Desaulniers, J.M.; Bajic, M. 2012. "TIRAMISU: FP7-Project for an integrated toolbox in Humanitarian Demining". *GICHD Technology Workshop* (September)

AUTHOR BIOGRAPHY

Geert De Cubber received in 2001 the degree of Master in Engineering at the Vrije Universiteit Brussel (VUB), with as specialization Electro-Mechanical Engineering. He then obtained a PhD. for his research in the field of 3-dimensional reconstruction of natural scenes perceived by mobile robots. This PhD. and the associated research project were part of a joined research effort between the Vrije Universiteit Brussel and the Belgian Royal Military Academy (RMA).
Currently, Geert De Cubber is a researcher working in the department of Mechanics of the Royal Military Academy, where he is leading the research activities of the research group on robotics for high-risk applications. The specialization of this research unit is the development of unmanned vehicles (aerial, marine and ground robotic systems) for high-risk applications like search and rescue and humanitarian demining. Within the group of Unmanned Vehicle Centre, Geert's main task is to apply computer vision techniques to mobile robots, rendering these robots able to perceive, analyse, and – to some degree – understand their environment. More specifically, three-dimensional reconstruction and cognitive vision approaches are investigated with the aim to port the capabilities of the human eyesight to intelligent robots
Currently, Geert is the coordinator of the EU-H2020-SafeShore project which deals with the development of novel detection system to cover existing gaps in the maritime border security system. The main focus of this project is to find detection means for small unmanned aerial vehicles (drones), which cannot be detected by present-day security installations.
Previously, Geert was the coordinator of the EU-FP7-ICARUS project which dealt with the development of unmanned tools (aerial, ground and marine robots) which can assist search and rescue workers to save human survivors after a major crisis (earthquake, tsunami, typhoon, shipwreck, …).