Industry considerations on

Security research priorities beyond 2020

3 April 2019
# Table of contents

**Executive Summary** .................................................................................................................. 3

A. **Introduction** ............................................................................................................................ 7

B. **Key technology trends with high and direct impact on security** .............................................. 10
   1. Artificial Intelligence ................................................................................................................ 10
      Opportunities .......................................................................................................................... 10
      Threats .................................................................................................................................. 10
      Capability gaps and research needs ...................................................................................... 11
      Strategic autonomy aspects ................................................................................................. 11
   2. Data Science ............................................................................................................................. 12
      Opportunities .......................................................................................................................... 12
      Threats .................................................................................................................................. 12
      Capability gaps and research needs ...................................................................................... 12
      Strategic autonomy aspects ................................................................................................. 13
   3. Autonomous Systems ............................................................................................................... 13
      Opportunities .......................................................................................................................... 13
      Threats .................................................................................................................................. 13
      Capability gaps and research needs ...................................................................................... 14
      Strategic autonomy aspects ................................................................................................. 14
   4. Augmented, Virtual and Mixed Reality (Immersive Systems).................................................... 14
      Opportunities .......................................................................................................................... 15
      Threats .................................................................................................................................. 15
      Capability gaps and research needs ...................................................................................... 15
      Strategic autonomy aspects ................................................................................................. 16

C. **Other security-relevant technologies** ..................................................................................... 16

D. **Conclusions** ............................................................................................................................. 17
Executive Summary

This paper provides industry’s recommendations for security research priorities under the Horizon Europe Framework Programme (2021-2027). To this end, it draws on the technological expertise and practical experience of ASD member companies.

We argue that the future security research programme should follow a twofold approach: First, ensure continuity of funding for certain security research areas of Horizon 2020, where additional or complementary work is needed to develop relevant capabilities. We see this need in particular in the areas of Cyber Security, Urban Security and Border Security. Secondly, address new breakthrough technologies which have an important security dimension. This forms the main part of this paper.

We divide these breakthrough technologies into two categories: First, technologies with potentially high and direct impact on a broad range of security areas. In this category, we include Artificial Intelligence, Data Science, Autonomous Systems and Immersive Systems. Security critical aspects of these four breakthrough technologies should be considered as a priority for the security research programme, since they can make a major contribution to the development of capabilities that are needed to fulfil the objectives of the Security Union (see table 1).

The second category are breakthrough technologies which can support certain security missions or imply security risks, but in rather limited fields of application. This second category includes Blockchain, Additive Manufacturing, Quantum Computing and 6G Radio Technology. We recommend covering the security dimension of these technologies not in the security research programme, but in other parts of Horizon Europe.

The four key technologies we recommend addressing in the security research programme post-2020 imply both security threats and opportunities, which we describe in the main part of the paper together with relevant capability gaps and research needs. Furthermore, we consider the security dimension of these technologies as so significant that a certain degree of non-dependence from non-European suppliers is crucial. The security research programme should therefore also aim to support Europe’s strategic autonomy at least on the most critical security aspects of these technologies (see table 2).

Finally, we advocate for a close coordination between the different components of Horizon Europe in order to cover the security dimension of the identified eight breakthrough technologies. Driven by the commercial sector, the latter develop at very high speed and may well lead to currently unexpected synergies and applications. Consequently, technologies that we consider today as less relevant for security may well lead tomorrow to results that can have a high impact on security. It is therefore of utmost importance to develop across different clusters of Horizon Europe a comprehensive approach towards the security dimension of all these technologies.
Table 1: Schematic process to identify technologies for security needs

<table>
<thead>
<tr>
<th>MISSIONS &amp; PRIORITIES</th>
<th>CAPABILITY NEEDS</th>
<th>THE PLAN</th>
<th>SUPPORTING TECHNOLOGIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protect people, public spaces and critical infrastructure</td>
<td>Predict, prevent and counter physical and cyber-attacks</td>
<td>Enhance interoperability between different surveillance systems</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>Support the use and protection of data flow for law enforcement</td>
<td>Prevent data theft and hacking</td>
<td>Enhance data storage, exchange, processing and analytics</td>
<td>Data Science</td>
</tr>
<tr>
<td>Support air, land and sea EU border management</td>
<td>Continuous detection, full protection and fast incident response</td>
<td>Improve detection &amp; monitoring of cross-border inflows of people and goods</td>
<td>Blockchain</td>
</tr>
<tr>
<td>Fight terrorism and radicalisation</td>
<td>Detect terrorist networks and stop their activities in time</td>
<td>Assess continuously terrorist risks and vulnerabilities</td>
<td>Quantum Computing</td>
</tr>
<tr>
<td>Prevent and fight serious and organised cross-border crime</td>
<td>Detect organized crime networks and stop their activities in time</td>
<td>Enhance public intelligence activities all over Europe</td>
<td>Artificial Intelligence</td>
</tr>
<tr>
<td>Prevent and fight cybercrime</td>
<td>Detect and stop cyber crime activities of private and public actors</td>
<td>Improve interoperability and trans-European information exchange</td>
<td>Data Science</td>
</tr>
<tr>
<td></td>
<td>Uncover cyber security gaps before malicious actors do</td>
<td></td>
<td>Blockchain</td>
</tr>
</tbody>
</table>

- Artificial Intelligence
- Data Science
- Autonomous systems
- Immersive Systems
- 6G
Table 2: Key technology trends and their importance for strategic autonomy

<table>
<thead>
<tr>
<th>KEY TECHNOLOGY TRENDS</th>
<th>STRATEGIC AUTONOMY FACTORS</th>
<th>FULL TECHNNOLOGICAL CONTROL</th>
<th>MINIMISING VULNERABILITIES</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARTIFICIAL INTELLIGENCE</td>
<td>Increasing importance of AI in security sensitive areas ⇒ need to fully control and master relevant AI technologies and algorithms</td>
<td>Increased probability of backdoor information security attacks (e.g. subversion of AI and machine learning systems) if provided by foreign third party ⇒ need to secure against attacks and misuse of technology via security-by-design and deliberate choice of suppliers</td>
<td>Need to develop and maintain in Europe a sovereign capability of secure and assured systems, algorithms and learning systems suitable for security applications</td>
</tr>
<tr>
<td>DATA SCIENCE</td>
<td>Need to have constraintless and reliable networks and processing as well as sovereign control of cloud based storage systems to harness the full potential of data analytics tools</td>
<td>Increasing significance of data storage, flows and management for security purposes, but data analytical tools vulnerable for backdoor attacks ⇒ need to have extremely secure data storage and management systems which are hard to attack or manipulate</td>
<td>Need for European companies to be able to equip security authorities with secure, reliable and state-of-the-art data science applications</td>
</tr>
<tr>
<td>AUTONOMOUS SYSTEMS</td>
<td>Autonomous systems rely heavily on secure data transmission &amp; autonomous control and may operate sensitive payloads ⇒ need to integrate these systems into a wider system</td>
<td>Autonomous systems can be remotely manipulated and used as surveillance systems by threat actors ⇒ reduce the risk for those attacks decreases with the trustworthiness of suppliers</td>
<td>Need for a strong industrial and technological base in Europe to master autonomous control systems, security sensitive payloads and data</td>
</tr>
<tr>
<td>IMMERSIVE SYSTEMS</td>
<td>Current dependence on non-European suppliers for Immersive Systems undermines the long-term security of supply for state-of-the-art equipment</td>
<td>Immersive systems can potentially be remotely manipulated or spied on ⇒ reduce the risk for those attacks decreases with the trustworthiness of suppliers</td>
<td>Immersive systems are currently being driven by American and Asian companies for the consumer market, putting at stake Europe’s technological expertise in this field ⇒ Europe needs to be able to apply/adapt these technologies and develop applications independently</td>
</tr>
</tbody>
</table>
A. Introduction

The purpose of this paper is to provide input for the strategic planning of the security research part of the next Research Framework Programme (Horizon Europe). It points out key technology trends that industry considers as crucial to fill the capability needs that derive from current security challenges and to reach the policy objectives of the Security Union.

Based on our assessment, we believe that the future security research programme should follow a twofold approach:

- **Ensure continuity**

Where appropriate, Horizon Europe should continue or complement certain security research actions that have been supported under Horizon 2020. We have identified the following three priority areas where this would be particularly useful:

1) **Cyber Security**: Future research projects should contribute in particular to improving situational awareness and protection against attacks on the cloud environment, Internet of Things, supply chains, and against cryptojacking of financial transactions;

2) **Urban Security**: To help protecting densely populated urban areas and critical infrastructure against man-made and natural disasters, future research activities should focus on protective measures, increased situational awareness and decision-making during fast evolving and dynamic events;

3) **Border Security**: Future research efforts should concentrate on enhancing the interoperability of surveillance systems between authorities from different Member States and the smooth exchange of information, but also on the improvement of detection capabilities for specific sensor technologies.

- **Address relevant new technology trends**

Most current breakthrough technologies are related to digitalisation and driven by the commercial sector. In particular large internet firms invest heavily in these technologies, which are likely to lead to profound changes in our societies and economies. Many of these technologies have also an important security dimension. In this context, we suggest distinguishing between key technology trends that can have a high and direct impact on security and other security-relevant technologies.

---

1 Technology Trends were drawn from a number of sources and publications including Forbes, Gartner, Interesting Engineering, Accenture, Finextra Research, Deloitte.
Key technology trends with high and direct impact on security

Some breakthrough technologies can have a direct and strong impact on a broad range of security areas. They can be used to develop specific security solutions or may be applied directly (or in an adapted form) for security purposes. At the same time, they can (often) also be used by wrongdoers for criminal or terrorist activities. We believe that the following four technologies are key for security and should therefore be covered in the future security research programme:

1) **Artificial Intelligence (AI)** yields great potential to significantly enhance the effectiveness of security relevant operations through the application of, among others, *smart solutions* and machine learning. At the same time, the same technology can also be applied by threat actors to provide targeted and more efficient attacks, including automated operational response and adaptation in the cyber and physical domains.

2) **Data Science** is crucial for a broad range of new security relevant applications and can help to anticipate, prevent and mitigate threats at a new dimension. From a threat perspective, such systems need to be resilient against information attacks. Data analytics could also be used by threat actors to plan attacks.

3) **Autonomous Systems** can provide improved surveillance and detection of borders and critical infrastructures and support first responders in unclear and dangerous situations such as natural disasters or terror attacks. However, if used with malicious intention, autonomous systems such as drones represent a new dimension of asymmetric threats.

4) **Immersive Systems** such as augmented, virtual and mixed reality can improve the operational efficiency of security authorities and first responders by better preparing them for their mission, enhancing situational awareness and facilitating decision-making in action. Yet, the same accounts as well for criminal or terrorist actors in preparation or during the execution of attacks.

The security dimension of these technologies is so important that **strategic autonomy** becomes critical and should be considered as an objective for future security research actions. The concept of strategic autonomy is admittedly as pervasive as it is vague. In technological terms, it implies a certain degree of non-dependence from non-European suppliers. In the above-mentioned key technologies, the security research programme should therefore aim at developing European sources of supply when there is a need for European end-users to:

- have full control of the use of a certain technology without restrictions or constraints from third countries or third country entities, for example to integrate it into a wider system (of systems) or adapt and modernise an application;
- rely on trustworthy suppliers for the protection of critical infrastructures and highly sensitive security systems, for example against hidden intrusion;
- ensure that the relevant industrial and technological competences and know-how are always available to maintain, operate and update a critical system.
Other security-relevant technologies

On top of the above-mentioned four key technologies, we have identified four other breakthrough technologies as security-relevant. These technologies have the potential to support certain security missions or can pose a threat in certain areas. At the same time, we consider them as less pertinent for the future security research programme, since we expect their field of security application to be relatively narrow:

5) **Blockchain Technology** can support security authorities when it comes to the storage of static information and secure exchange of information, yet wrongdoers can use the technology to secretly plan and execute attacks.

6) **Additive Manufacturing (AM)** enables cheaper, faster and customised production of equipment but brings along the risk of home-made weapons or explosive devices.

7) **Quantum Computing** has the potential to dramatically boost computing performance, enabling more secure encrypted communication and high-speed big data search. Yet, this new computing dimension also creates risks in terms of data security and hacking attacks.

8) **6G Radio Technology** would allow for a new generation of mobile data communication, greatly facilitating the work of security authorities and first responders in action. However, given the vast amount of, often sensitive, data transmitted via 6G components, the imprudent choice of suppliers could create huge vulnerabilities to critical infrastructures in Europe.

In spite of their security dimension, we believe that this second category of technologies should not be considered as a priority for the security research programme, but rather be supported by other parts of Horizon Europe, in particular within the cluster ‘Digital and Industry’. At the same time, all technologies are closely intertwined and interdependent. Research programmes and funds should therefore emphasise coherence and coordination across the different clusters of Horizon Europe in order to ensure a sustainable and useful outcome.

In the following, we will elaborate in greater detail the security aspects of the four key technology trends that the future security research programme should directly address. We will look in particular at their:

- Opportunities and threats;\(^2\)
- Capability gaps and research needs;
- Strategic autonomy aspects.

We will then do the same exercise in less detail also for the second category of other security-relevant technologies that should be supported through other EU funding programmes.

---

\(^2\) To keep this paper unclassified the threats posed have been kept at a very general level.
B. Key technology trends with high and direct impact on security

1. Artificial Intelligence

Intelligent systems use Artificial Intelligence (AI) and machine learning to interact in a more intelligent way with people and their surroundings. These systems can operate semi-autonomously or autonomously in an unsupervised environment to complete a particular task. Increasing computing power and availability of data sets have been crucial to enable advancements in AI.

Opportunities

The use of intelligent surveillance systems is perfectly suited to support human operations and increase efficiency in security relevant fields. For first responder operations, for example, AI can help to establish reliable early warning systems through data collection, optimised algorithms and machine learning. This supports decision makers in taking early and appropriate action. Medical treatments during operations may also be enhanced with the use of specific AI applications. For border management, solutions such as the ’Smart Gate’ provide reliable 24-hour surveillance, enabling law enforcement authorities to control borders more efficiently and spot security risks earlier. Similarly, AI is also an enabler for secret services or law enforcement authorities in gathering and analysing intelligence and can be used to enhance surveillance and protection of critical infrastructures.

Threats

The increasing dependence on intelligent and interconnected technology, as well as the proliferation of adversary tools to exploit vulnerabilities in systems and networks create new security risks and threats:

- **Information security attacks on intelligent systems** have the potential to disable critical infrastructures or border management systems;
- AI could be used to provide **automated response and attack**, both at the cyberwarfare level or physically through the use of weaponised drones and other platforms. Since AI can be applied with ever less components and ever smaller devices (based on chip solutions and micro-electronics), this threat scenario will become more significant in the coming years;
- **Privacy and data protection** are at stake as a growing amount of data is collected by public authorities and private firms with the use of AI tools. Data leaks and cyberattacks can result in sensitive data falling into the hands of hostile states or organisations;
- **Machine made decisions based on AI technology** may pose a threat if a machine takes a **wrong decision** resulting from erroneous information without a human being having the possibility to intervene. This could affect border and airport controls, the surveillance of mass events or provoke false alerts in critical infrastructure.

To mitigate threats posed by AI, **security by design** is a key requirement. One example of such a pre-emptive measure is ensuring state-of-the-art (cyber) security resilience from the earliest
stage of the product cycle. This includes permanent monitoring of potential attacks and the ability to adapt and maintain security controls for intelligent systems accordingly in real time, without disrupting operations.

**Capability gaps and research needs**

AI systems in the consumer domain are already relatively mature. In fact, some AI applications already exceed human capacity in some fields such as image recognition. With a view to security applications, further research seems necessary to develop the following capabilities:

- **Sufficient integrity and robustness.** Whilst a consumer unit can tolerate mistakes, a system used for security applications cannot tolerate false alarms and alerts as it has the potential to cause considerable material and personal damage;
- **Assurance of AI systems against their required concept of operations.** This includes how AI applications are trained for security critical applications or integrated into existing technical schemes and the relationship between safety and security;
- **Correct and reliable interpretation of data** collected by AI systems to avoid technical dysfunctions;
- **Usability and integration in productive environment with legacy systems.** Intelligent systems and AI improvements need to be seamlessly integrated into existing software environments owned by security authorities in order to maximise the chances for rapid uptake of the technologies;
- **Improved human machine interface** to ensure the relationship between AI solutions and the human operators is efficient and compatible;
- **Autonomous search and repair of vulnerabilities against cyber security attacks;**
- **Predictive analysis** for the forecast of potential cyberattacks, crime and terrorist attacks;
- **Dynamic risk management** for the integration of information across domains, e.g. critical infrastructure protection;
- **Consideration of the ethical dimension of AI** in security applications in general.

Combined, these steps would significantly improve the design and deployment of AI for security, while maintaining the integrity and reliability of intelligent unsupervised surveillance systems to support human operations.

**Strategic autonomy aspects**

AI and algorithms on which it is based will become increasingly important for a broad variety of key security applications. It will be used for surveillance, intelligence or threat assessment prediction, in sensitive areas such as the protection of borders, critical infrastructures and digital security. Given the importance and sensitivity of these security applications, it is crucial for Europe to have its own AI sovereign capability to develop the necessary algorithms and solutions, as well as to operate and maintain the relevant secure and assured systems.
2. Data Science

This technology is based on the use of big data as a means to assess certain developments and adapt possible actions accordingly. In security, advanced analytics can use big data to better predict future security risks, both in the digital and the real world.

Opportunities
Advanced analytical data systems can help to anticipate the evolution of possible threats and to define the appropriate reaction. This can greatly improve for instance the prediction and monitoring of information security attacks, the reliability and accuracy of sensor systems or the prediction of natural disasters. Moreover, border security and flow management can be improved thanks to the use of automated multi-modal biometrics based on highly sophisticated data analytics and science techniques. Eventually, data analytical systems have the potential to improve considerably the performance of criminal and forensic analysis through new data science techniques which would result in a more robust and enhanced law enforcement.

Threats
The use of data analytics and science technology bears important security risks, in particular by increasing:

- **The impact of information attacks on security-relevant applications** in fields such as cloud-based systems, supply chains or the Internet of Things;
- **The capability of threat actors to provide more targeted attacks**, as for example all civil aircraft have transponders that anybody can monitor. Data analytics could therefore be used to analyse and plan attacks;
- **The impact of data theft** for both private users and public authorities. Data theft from security agencies in particular is a considerable security threat as it risks revealing highly sensitive information to criminal or terrorist actors.

Resilience to such attacks needs to be a top priority already in the research and development phase. Even though the threat scenarios described above are not new as such, they will reach a new dimension in the next years due to the sheer amount of data that will be collected, stored and used. This will enable wrongdoers to use big data actively as a means and to multiply at the same time potential targets.

Capability gaps and research needs
Data science and data analytics are already being widely used in the commercial and military domains. Research is ongoing particularly in the cybersecurity domain. For instance, H2020 has a call in 2019 concerning information and data stream management in fighting cybercrime and terrorism. Future capability gaps of advanced data analytical systems are likely to appear in **safety and security related applications** (e.g. during natural disaster operations). Research needs will be **similar to those identified above for AI technologies** (except autonomous search and repair of vulnerabilities against cyber security attacks).
Strategic autonomy aspects
Data analytic tools are indispensable for security threat prediction and surveillance supported by the necessary monitoring, scanning and response systems. The growing number of connected devices and deployed unmanned systems will constantly increase the amount of data that security authorities can use for that purpose. At the same time, data analytical tools can be vulnerable to ‘backdoor’ attacks (e.g. spy activities, data breaches or subversion of systems). Consequently, it is of strategic importance to maintain an industrial and technological base that is able to equip European security authorities with secure and reliable products made in Europe.

3. Autonomous Systems
The driver of this technology is the private sector, developing for example commercial drones (e.g. for sport and cheap video surveillance) or autonomous cars. Autonomous systems and vehicles are also being developed for the defence and security sector.

Opportunities
Autonomous systems can be used with different functionalities for multiple purposes and in all domains. They have for example the potential to play a significant role for border control and response to incidents. 24/7 all-weather autonomous surveillance systems can greatly improve situational awareness. Autonomous systems and vehicles are also promising enablers for search and rescue operations and can provide first responders with much better means for remote surveillance and standoff detection.

Threats
The remote steering or control of autonomous systems and their increasing capacities in terms of distance, duration, precision and payload opens new possibilities for threat actors. The use of AI will increase this further, making it possible for example to use swarms of drones for malicious intent. Examples of current and emerging security threats are:

- Commercial drones to deliver CBRe and other payloads;
- Autonomous drones including swarms of vehicles as an attack means;
- Commercial drones to provoke collisions with aircraft or spoof vehicle movement;
- New automated vehicles for smuggling arms, drugs or people;
- Information attacks on future autonomous cars and air transport.

To reduce the threat from malicious drones, it is key to develop and establish as early as possible a European wide accessible and personalised (‘one drone, one person’) registration platform for drones (or certain types of them). In parallel, counter drone technologies (detection, identification, mitigation, response) need to be developed (see below). Transport systems have to increase their cyber resilience to prevent cyberattacks on autonomous vehicles.
Capability gaps and research needs

In this domain, several security- and defence research programmes are ongoing at the European and national level. Such programmes focus on counter-drone technology and the use of autonomous systems in operations. Counter-drone systems have already been deployed in military and civil security environments for protection at mass events. However, a major capability gap remains the reliable detection, identification and neutralisation of malicious drones. It remains a challenge to distinguish them from harmless drones or birds without disrupting normal operations (e.g. not interfering with emergency services communication bands). Additionally, autonomous vehicles do not yet run flawlessly and still have some technological room for improvement.

To this end, research needs for autonomous systems are as follows:

- Improved sensors capabilities to enhance the functioning of autonomous operation in harsh environments;
- Better detection capabilities (especially for small objects) supported by sensors equipped with AI methods and tools;
- Better affordability and usability of drones in urban environments or densely populated areas;
- Enhanced counter drone tools that are compatible with spectrum requirements;
- Due to the current legislation constraints for drone flights in populated areas, a special focus should be put on manned-unmanned teaming as a viable and pragmatic way to progressively support the insertion of fully autonomous unmanned platforms in real operations;
- Improved endurance and resilience for all operations and environmental requirements.

Strategic autonomy aspects

Autonomous systems will depend on the transmission of data that need to be secure and reliable in order to ensure that the systems operate safely and securely and will operate sensitive payloads. Consequently, Europe should maintain a certain autonomy as to the development and protection of relevant data links, and sensitive payloads used for surveillance and response operations. In order to at least diminish the risk of attacks, the virtual control of autonomous systems should be based on reliable sources from Europe.

4. Augmented, Virtual and Mixed Reality (Immersive Systems)

Augmented reality (AR), virtual reality (VR) and mixed reality (MR) are changing the way people perceive and interact with both the digital and the real world. They do so via their capacity to provide additional real-time information transmitted by specific high-tech glasses to the user with regards to the surrounding environment or by even simulating this environment in a different local setting (e.g. in a VR training centre). Real-time image processing has reached a level that was unimaginable a few years ago and is continuously advancing. Combined with voice recognition systems and haptics platforms, this will fundamentally change the way the user operates in his - nearby or remote - environment. The driving actor for these technologies is first
and foremost the private sector. The lines between consumer tech and security and military hardware are, however, ever blurrier. One example is Microsoft’s holographic computer ‘Hololens’ which is being supplied to commercial customers and to the U.S. army.

Opportunities

Immersive systems such as head worn displays are especially promising to support first responders. They can, for example, provide improved visualisation of hazards, improved situational awareness, hands free operation and be used to provide information for triage at an incident. Topographical data can be relayed along with video feeds from remote overhead drones or other first responders nearby, with a 360-degree view of the field of action. This decreases cognitive loads and stress levels and facilitates decision-making by allowing to filter and sort information. Another opportunity relating to immersive systems is the provision of telemedicine type information to responders that are at the scene before medical personnel arrives. Last but not least, immersive technology can also be used in training and simulation to prepare for ‘low probability, high impact events’ such as terrorist attacks.

Threats

The technological upgrading of immersive systems also brings along a number of threats such as:

- The possible use of consumable and wearable technology with integrated immersive systems technology by terrorists or criminals;
- Hacker attacks on immersive systems, which are especially harmful when mostly needed, for example during a police or civil protection operation;
- Sensor failures sending wrong signals to the machine or human in charge, resulting in erroneously informed decision-making and possible collateral damage.

The gradual enhancement and reliability of sensors and techniques used in immersive systems is crucial. A high technical standard of protection for all types of immersive systems needs to be ensured at all times and needs further research.

Capability gaps and research needs

A considerable amount of research and development is being conducted at international and national levels on wearable technology for AR, VR or MR. The commercial industry is the primary driver in such developments. Under H2020 and FP7, immersive systems have been developed in projects such as AUGMED.

The main capability gaps of immersive technologies for security concern deployability. Immersive systems must be capable to operate in all environmental conditions, be rugged, lightweight and compatible with any of the first responder systems, e.g. respirator system. Displays must have improved human interfaces to ensure full situational awareness and provide the most appropriate information at the correct time. Moreover, they must be easy to upgrade and integrated at low cost. Consequently, further research efforts are necessary to enhance display technology, the visualisation of data, as well as the combination of multiple sources of
information and data in action. Robust training programmes are necessary to prepare and accompany the progressive insertion of these systems in real operations.

**Strategic autonomy aspects**

The commercial market for immersive systems is clearly dominated by the United States and Asian countries. Most of immersive technology building blocks are therefore developed by non-European entities, which means that supply and maintenance are out of European control. As a consequence, immersive technologies might not be delivered to European security authorities suitable for operations or training purposes. Moreover, dependence on non-European sources can come along with the risk of remote manipulation or spy attacks against immersive systems. For all these reasons, Europe should make an effort to develop immersive security applications and maintain its own capacity to produce or partner to further develop immersive systems for security (and defence) purposes.

**C. Other security-relevant technologies**

1) **Blockchain** is an application that can support security authorities via its two fundamental functions, i.e. record keeping (the storage of static information) and transacting (registry of tradeable information). Highly sensitive data for critical infrastructure or intelligence activities can be encoded and protected. On the other hand, the same accounts for criminal or terrorist groups which can use Blockchain to plan and execute attacks, both digitally and in the real world. More research is required to improve compatibility aspects and seamless integration in decentralised distributed blockchain systems, blockchain as a service (BaaS) and the application of permission-less and permissioned blockchain.

2) **Additive Manufacturing (AM)** uses the method of joining materials in an automated process to create objects from 3D model data, usually layer upon layer. This allows for a cheaper, faster and tailor-made production, also of security relevant equipment. On the other hand, the ‘democratisation of manufacturing’ through AM implies also the possibility for basically everyone to produce weapons and other malicious tools, which creates a completely new form of asymmetric threat. To better use AM for security equipment, more research is needed on the hardware side (better materials such as polymers and special machines for ‘sintering’) and on the software side (Computer-Aided-Design and data storage managing).

3) **Quantum Computing** uses quantum bits accelerating computing performance many times over. This can make coordination between security forces sharing cryptographic keys quicker and more reliable. Large data bases can be searched through much faster, e.g. to find criminals, but also encryption strategies of malicious organisations can be detected more easily. In turn, quantum computers have the potential to render many of today’s most sophisticated encryption systems useless. This affects both public and private data storage systems and can become a major threat to digital government networks and financial
systems. From a security perspective, additional research is needed to develop and deploy encryption systems that can withstand a quantum attack.

4) **6G Radio Technology** will bring along an enormous densification of data flows in communication systems, enabling thousands of simultaneous wireless connections. This would result in global coverage, higher capacities and always-on connectivity. In turn, this represents the base for reliable and low-latency application of intelligent, immersive and autonomous systems. 6G therefore yields great potential to support the work of security authorities and first responders in action (in terms of communication and data processing). However, it is exactly this massive flow and storage of, often highly sensitive, data that creates vulnerabilities to possible spying, hacking or manipulation attacks. To secure 6G know-how in Europe, more research is for instance needed on how to cope with ever smaller wave lights and their resilience against possible obstacles, but also with regards to better protecting critical communication infrastructure against cyber-attacks or natural disasters (e.g. via the full integration of Public Protection and Disaster Relief, enhanced satellite communication as well as the ability for fast reconfigurability and orchestration of services).

### D. Conclusions

The technology trends presented in this paper demonstrate to what extent technological transformations can shape security in both a positive and negative way. Yet, more research is needed to harness the opportunities which those technology trends offer and to mitigate their threats. Summing up the key findings of this paper, ASD recommends the following guiding principles for the security research programme post-2020:

1) **Ensure continuity and avoid disruption**: Positive examples of successful projects funded under Horizon 2020 are numerous. Some priorities such as urban-, cyber- and border security should therefore be continued and transitioned into Horizon Europe to guarantee continuity in security research.

2) **Address breakthrough technologies that will strongly impact security**: Security research cannot be based on a scattergun approach but needs prioritisation. AI, Data Science, Autonomous Systems and Immersive Systems represent from our point of view four key technology trends that will be highly relevant for security and should therefore be addressed in the future security research programme. This requires long-term programming and investment planning from basic research to development. For higher TRLs, roadmaps must be established and tailored towards specific capability needs.

3) **Consider the security dimension of other technologies**: The security research programme should cover only the most security-relevant technologies. At the same time, the possible security dimension of other breakthrough technologies should not be neglected and addressed in other clusters of the future Framework Programme. This makes it particularly
important to ensure strong cooperation and coordination between the different programmes of Horizon Europe. As part of the strategic programming for Horizon Europe, the EU should scan all breakthrough technologies for possible security implications. Doing such a scan at an early stage of the technology cycle would allow to tailor research efforts proactively, rather than reactively as it has been the case up until now (for instance with regards to ATM or 5G).

4) Secure Europe’s strategic autonomy: Some key technology areas are so critical for security that Europe should not completely depend on non-European suppliers. The security research programme should therefore aim to reach a certain level of strategic autonomy in the most sensitive areas. This does not exclude cooperation with third countries, particularly on the definition of requirements, processes or best practices. However, in order to ensure the security of its citizens, the EU should be able to control the technologies used to fulfil these requirements and to implement these processes and practices.

To develop the industrial and technological base for the European Security Union, a more strategic approach is needed. The security research programme should include a broad range of instruments that allow to react at the same time to emerging technology trends (long-term) and against pop-up threats (short-term). It should be built on an effective link between policy decision-makers, practitioners, industry and academia. Furthermore, a capability planning process should be established at the European level to overcome the fragmentation of security needs and thereby facilitate the market uptake of European security products.

ASD is delighted to give a first input for the initial phase of the security research programme with this paper. We stand ready to further contribute with industry’s technical expertise and practical business experience to make the future security research programme a success.

****

Signed by Jan Pie, ASD Secretary General, on 3 April 2019

About ASD

ASD is the European Association of aerospace and defence industries in Europe, representing more than 3000 companies from across Europe. We are the key interlocutor of the European institutions and agencies on industrial aspects of defence and security. So far, ASD has provided input, for example, for the preparation of the Internal Security Fund and previous security research programmes.

The leading ASD body on security matters is the Security Business Unit (SBU). The SBU brings together 20 high-level industry representatives from our member companies and associations all over Europe and has collaboratively elaborated this paper.

Contact

Burkard Schmitt
Defence & Security Director, AeroSpace and Defence Industries Association of Europe
Burkard.Schmitt@asd-europe.org
T : + 32 2 775 81 30
M : + 32 4 7143 93 19
Rue Montoyer 10, 1000 Brussels, Belgium