EU High-Level Informal Seminar
Threats and opportunities of emerging technologies in the field of security

thecamp | 2-4 April 2019

Rationale:

At the request of the European Council of October 2017[1], the Commission published, in April 2018, a first European approach to Artificial Intelligence (AI)[2]: it recognised the EU's lag in this area and proposed it should build its own model, where the race for innovation would meet EU values (data protection and a high level of digital rights and ethical norms), and based on three pillars: ensuring an ethical and legal framework, encouraging the generalised use of AI in industry and preparing for the socio-economic transition. In December 2018, the Commission presented a Coordinated Plan on AI with the Member States in order to launch specific actions as of 2019-2020[3] at the request of the European Council of June 2018[4].

Whereas communications on AI tend to identify security as one of the industrial sectors where the EU is leader and one of the key implementation areas where it is worth investing and promoting its use, **there isn't a consolidated European vision on the risks and opportunities of technological innovation in the field of security** (and, by extension, in the area of Defence), which would allow EU efforts to converge in an ambitious security policy responding to citizens' needs.

In parallel, the Commission has a number of initiatives to support innovation in Europe, mostly in collaboration with Member States, in areas such as completing the digital single market, cybersecurity, blockchain, facilitating access to finance, research or protecting investment. More such initiatives have been proposed for the next MFF (2021-2027)[5].

In the context of our growing exposition to risk due to our dependency on foreign technological infrastructures and the increasing digital interconnection of the business, private and public spheres, the advantages that new technologies offer both the security services of the Member States and their adversaries (other countries, criminal organisations, political groups, terrorist groups and their proxies), force us to reflect specifically on this issue, to ensure that the EU's approach to AI and related policies are fully in line with autonomous European security policy.

As a follow-up of the sessions on AI and blockchain organised by the EU CTC in Brussels in September 2018, this high-level European seminar at thecamp, a campus in the South of France dedicated to positive innovation, will allow us to better **understand the opportunities and threats offered by new technologies,** to analyse how **to boost EU security agencies to in their use of new technologies to benefit to member States,** to **identity pilot projects** and to

[1] European Council conclusions of 19 October 2017.

[2] Communication COM(2018) 237 final of 25.4.2018 'Artificial Intelligence for Europe'.

[3] Communication COM(2018) 795 final of 7.12.208 'Coordinated Plan on Artificial Intelligence' and its Annex.

[4] European Council conclusions of 28 June 2018.

[5] The Commission's plans to dedicate around nine billion Euros to the Digital Europe Programme in 2021-2027, including 2.5 for AI, 2.0 for cybersecurity and 2.7 for high-performance computing.

reflect on how to mitigate the obstacles and to harness the levers for an **EU technological leadership and autonomy in the field of security**.

Location:

Inspired by American campuses, start-up accelerators and fab labs, **thecamp (https://thecamp.fr)**, was initiated in 2013 and is located in Aix-en-Provence, in natural surroundings. Its mission is to bring people and projects together in order to explore new sustainable and collaborative approaches to global issues (oceans, mobility, education, food, cities, quality of life) in a nurturing environment. Both private companies and public entities provide financial support.

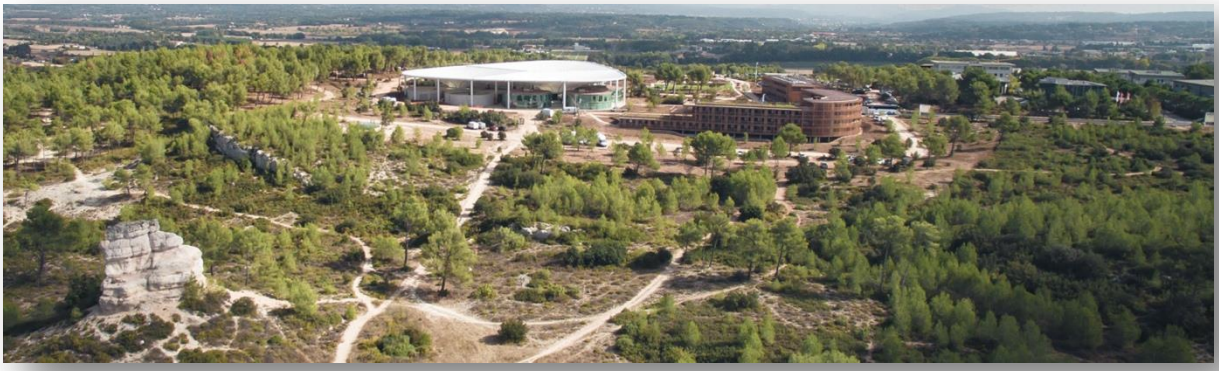
thecamp offers a wide range of activities to suit different needs and profiles:

- **education and facilitation**: in order to address the challenges related to innovation, transformation, collective intelligence and the appropriation of emerging technologies, thecamp proposes training programs, stimulates creativity and organises custom-made activities.
- **support for projects through incubation and experimentation**: A 6-month collaborative residency program (20 young artists and creators from all over the world explore and hack the future, developing concrete solutions to global problems); experimentation (testing, on the field and in real-life conditions, of innovative ideas, such as future train stations or urban mobility); acceleration and incubation programmes for start-ups; a workshop providing tools and software, including 3D printing, to design and create prototypes (the "fablab"); and bringing together major groups, NGOs, politicians, artists, militants, public citizens, children to work together on projects with a collective impact, for example stopping ocean pollution or proposing innovative transport solutions for the future ("waves").

thecamp welcomed 30 000 people in 2018, meaning an average of 2 500 visitors per month.

The building has been designed by Corinne Vezzoni, an architect from Marseille.

Since May 2018, Olivier Mathiot, cofounder of PriceMinister, is the non-executive President.



thecamp
550, rue Denis Papin
La Duranne
13100, Aix-en-Provence
France
Geolocation: 43.497505,5.341912

Programme

Tuesday 2 April 2019 - Understanding the use of technologies in security

Arrival at thecamp - *Check-in*

13:15-14:15 Lunch ***1st Floor Restaurant***

Welcome words by thecamp (Julie Thinès)

14:30-15:30 Global overview of technologies ***Room : Inspire Lab***

Welcome words by Gilles de Kerchove

Speaker : Gilles Babinet

15:30-18:00 Imagining the future of (in)security ***Room : Inspire Lab***

Design Fiction by Nicolas Minvielle and Martin Lauquin

Method: Design fiction is a method increasingly used by organizations to imagine, model and test their future by using science-fiction imagery, cinema or literature. When we can foresee where we will be in 20 or 30 years, we can anticipate what we need to attain our objectives.

Objective:
1) to reflect freely on future disruptive technologies and on the transformations of organisations (public, private, societal) driven by innovation;
2) to focus specifically on present and future threats (crime, terrorism, threats to our sovereignty, social manipulation, etc) and on new ways of providing security (malicious use of AI, police, border control, space, next web, etc).

18:00-18:15 Break

18:15-19:45 Threats and opportunities of technologies for security ***Room : Inspire Lab***

Objective: To understand:
1) the deep transformations driven by technologies
2) potential developments and convergences (AI and cyber, AI and blockchain, quantum computing and satellites, etc)
3) possible use of technologies by security forces and their opponents (biometrics, facial recognition, drones).

18:15-19:00 Risks and opportunities of technologies in cybersecurity

Speakers : Nicolas Arpagian (10') - Julien Gadanho (10') - François Dellacherie (for discussion)

19:00-19:45 Risks and opportunities from Quantum Computing

Speaker : Olivier Ezratty (30')

19:45 Social event

20:30 Dinner (buffet) with speakers ***1st Floor of Restaurant***

Wednesday 3 April 2019 - Obstacles to an autonomous European security Union

07:30 Breakfast ***Restaurant***

08:30-13:30 Identifying technologies for security needs ***Room: Studio 1***

Objective of the morning session: Identify technologies capacities/usages and projects to respond to current and future security needs.

08:30-08:40 Briefing on methodology (Cristina Lagane and Julie Thinès)

08:40-10:30 Artificial intelligence

How Might We?

- Respond to AI enabled threats?
- AI be used to increase citizens security (Big data, predictive police, cybersecurity, fight against terrorist financing, facial recognition…)?
- Question: Which impact on security jobs and security paradigms?

Speakers (1h) : Olivier Ezratty (15'), Arnaud Guérin (Earth Cube - 15')

Brainstorming in groups (40')

10:30-11:30 5G and IoT

How Might We?

- Leverage 5G to support the security goals
- Monitor the limitations of 5G applications for security purposes (lawful interception, evidence availability, anonymity…)?
- Mitigate and respond to 5G enabled threats (deep fake, drones…)?

Speakers (1h) : Olivier Ezratty (15'), Ian Levy (Technical Dir. UK's National Cyber Security Centre - 15')

11:30-12:00 Break

12:00-13:00 Blockchain

State of art, last trends (consensus, side-chain, off-chain, scalability)

How Might We?

- Mitigate and respond threats and vulnerabilities
- Develop use case for security needs (to fight against terrorist and extremism online? To offer a credible and affordable payment transfer system for remittances as an alternative to hawala-type informal ones? To fight against illicit trafficking of cultural goods in view to finance terrorism?); use case (diamonds, WFP, payment transfers, remittances)
- Anticipate impact on security services

Speakers (1h) : Pablo Vallès (Consensys - overview 10'), David Fay (TheCoinHouse - finance 10'), Stone Atwine (Eversend - remittances Africa 10'), Gustav Strömfelt (WFP - Building blocks 10')

13:30-14:30 Lunch ***Restaurant***

14:30-19:30 The main challenges for technological autonomy in the field of security ***Studio 1***

Objective of the afternoon session*:* Identify the main obstacles and levers in using technologies to reach the autonomy of the EU in the security field.

14:30-16:00 Turning EU agencies into centres of excellence on technologies

Agencies in the field of Justice and Home Affairs (Europol, Frontex, Eurojust, CEPOL, ENISA, EDA, SATCEN) are already technological platforms that benefit Member States. What are their current technological capacities and tools? What are their objectives on the mid and on the long term? Which roadmap to reach the objectives?

Some questions arise:

- How should innovation be organised and encouraged? What profiles are needed? How should managers be trained? How can we foresee future talent needs?
- In which areas do they need to be reinforced? (biotechnology, terrorist, financing, supporting cyber research in areas such as dark web and cryptocurrencies, detection, protecting the EU's external borders, facial recognition, CBRN)
- Accessing and analysing data: How can we better analyse existing data? What hurdles need to be overcome to develop partnerships with the private sector for the exchange of data in order to fight against crime and terrorism?
- How can we better connect agencies to research projects in their earliest stages, including in the fields of military and spatial research, and production of industrial products?
- What security data infrastructures need to be set up in the EU to avoid depending on US platforms and avoid duplicating efforts?

Speakers (45') : Arnaud Guérin (Earth Cube) - André Loesekrug-Pietri (Jedi)

Brainstorming in groups (40')

16:00-16:15 Break

16:15-17:35 The impact of privacy regulations and ethics

The EU has chosen a well regulated technological model that adapts to its values (data protection, ethical norms, public-private partnerships with companies to access their data). How is it compatible in practice with development and use of technologies for security needs?

Some questions arise:

- Do the EU privacy laws/fundamental rights/ethical principles impede innovations in the field of security? Is it possible to develop an AI less dependent on personal data?
- Some concrete cases (WHOIS, KYC, PPP…).
- How ensuring access to enough data for security needs? Agreements with third States could be opportunities?
- Is it possible to reconcile security, safety and privacy by design? What kind of legal flexibilities could we exploit?
- How to implement transparency/explainibility of algorithms (bug bounty like in cybersecurity?)? Which impact of bias limitations (religious radical commitment, etc)?

Speakers (1h) : Audrey Decima (Avocate au Barreau de Paris), Raphaël de Cormis (Dir. innovation Gemalto), David Fay (TheCoinHouse)

Brainstorming in groups (20')

17:35-18:00 Break

18:00-19:45 Technological convergence and autonomy in the field of security ***Studio 1***

18:00-19:00 Risks and opportunities of technologies in specific sectors

Speakers (1h) : Henry de Roquefeuil (spatial), Thomas Landrain (biotech)

19:00-19:45 : Brainstorming in groups (45')

- Technological convergence: how can the EU integrate/articulate its different sectoral initiatives like digital single market, cybersecurity, defence, dual civil/military technologies, spatial development, AI and blockchain?
- EU technological autonomy: could Europe be independent from US and Chinese technology? Which technologies should the EU invest in to lead ('Palantir' type…)? How create a European Space for data for security? How can we link EU research policy to real security and operational needs? How can we cut red tape and adapt to the speed of new technologies and realities on the ground? How can we protect the results of EU research? What is the operational outcome of H2020? What public procurement policy (Buy European Act for digital security)? How can we better support start-ups & SMEs? Which EU instruments can encourage the creation of clusters dedicated to innovation in security? What education policy is needed to train and attract tomorrow's talents? What kind of other flexible instruments use or invent?

20:00 Informal dinner ***Restaurant***

Thursday 4 April 2019 - Operational out-takes

07:30 Breakfast ***Restaurant***

08:30-10:30 Next steps ***Room: Studio 1***

- Presentation of the main conclusions of the workshops
- Plenary discussion
- Conclusions: Gilles de Kerchove

10:30 End of the Seminar

With our thanks to the sponsors who made this seminar possible:

EUROPOL

FRONTEX
EUROPEAN BORDER AND COAST GUARD AGENCY

CEPOL

ISS EUROPEAN UNION Institute for Security Studies