



EDITO



Shaping Europe's digital future

by General of French armed forces (2S) Marc Watin-Augouard, Director of the CREOGEN

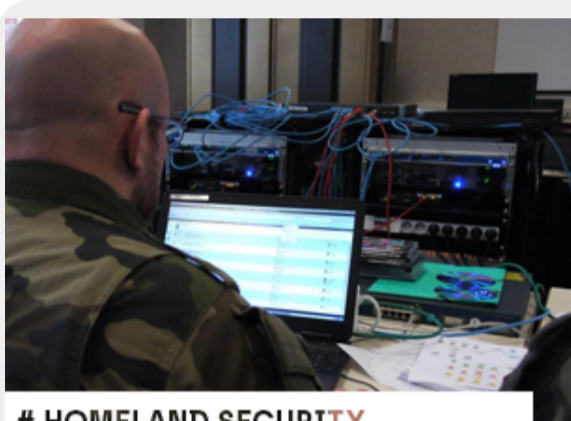
Digital Europe was initially designed to serve the development of the Single Market. But recently, sovereignty and cybersecurity have become two of the Commission's objectives in a strategic context marked by the domination of the two digital superpowers, the United States and China.

Yet Europe does not lack assets. It still lacked a unified and ambitious discourse, followed by effective action sustained over time. In March 2021, the European Commission showed the way by launching its "Digital Decade" programme. Cybersecurity has an essential place in this strategy. It is both its cornerstone and spearhead...

[Read the edito](#)

CYBER

INFO



HOMELAND SECURITY AND DEFENCE

Maritime cybersecurity: civilian and military sailors embark on new challenges

Like many other sectors, the maritime sector—which is diffuse and complex—is continuing its digital transformation. It is not immune to the proliferation of vulnerabilities that are all the more difficult to apprehend because ships and their equipment are heterogeneous, often inaccessible, and have a very long lifespan...

[Read the article](#)

LEGAL ISSUES

State sovereignty and blockchain

The applications of blockchain are multiple. If the monetary aspect is by far the most advanced and covered by the media, the technology makes it possible to go beyond the mere cryptocurrencies.

It is indeed sovereignty in the broadest sense that could be disrupted by this technology...

[Read the article](#)

CYBER CRIMINALITY

Vulnerabilities: the central issue of governance

Vulnerability researchers present very disparate realities—from simple enthusiasts to true professionals and to criminal organisations. How are the vulnerabilities they discover processed and exploited? What is the role of brokers? And what governance applies to this sometimes very lucrative activity? Is it effective at the international level?

[Read the article](#)

DIGITAL TRANSITION

China, the all-out offensive

5G networks, standardisation, proposal for a new internet...

For several years, China has been multiplying international initiatives in the fields of digital technology and cybersecurity.

An "all-out" activism that responds to a well-organized strategy and to clearly identified needs...

[Read the article](#)

FIC

NEWS



FIC 2022: 1st meeting of the Scientific Committee!

The first meeting of the Scientific Committee was held on Tuesday, October 5. The exchanges focused on topics related to the major themes of the FIC (legal issues - anti-cybercrime - cyber-risk management - homeland security and defense - operational security - digital transformation), and in line with the theme of this 2022 edition. The next meeting of the Scientific Committee will be held at the end of November / beginning of December.

FOLLOW US!



TÉLÉCHARGEZ

L'ÉDITION SPÉCIALE CYBER

face au RISQUE

[faceaurisque.com](#)

SAVE

THE DATE

Breakfast / Webinar: " Quantifying cyber risk: anticipate and measure to better protect yourself "

October 28, 2021

Beyond their direct, visible and tangible impacts (operating difficulties, paralysis of systems or loss of data leading to a slowdown or stoppage of production,...), cyber attacks or incidents also have indirect consequences and costs, sometimes hidden but always difficult to apprehend: damage to image and/or reputation, drop in financial value, contractual penalties with suppliers or customers...

[I register!](#)

INCYBER PARTNERS

Contact : contact@incyber.fr

Avisa Partners - Tour Montparnasse - 33, avenue du Maine, 75755 Paris Cedex 15 - FRANCE

inCyber

The media hub of the FIC community

[Unsubscribe? click here](#)