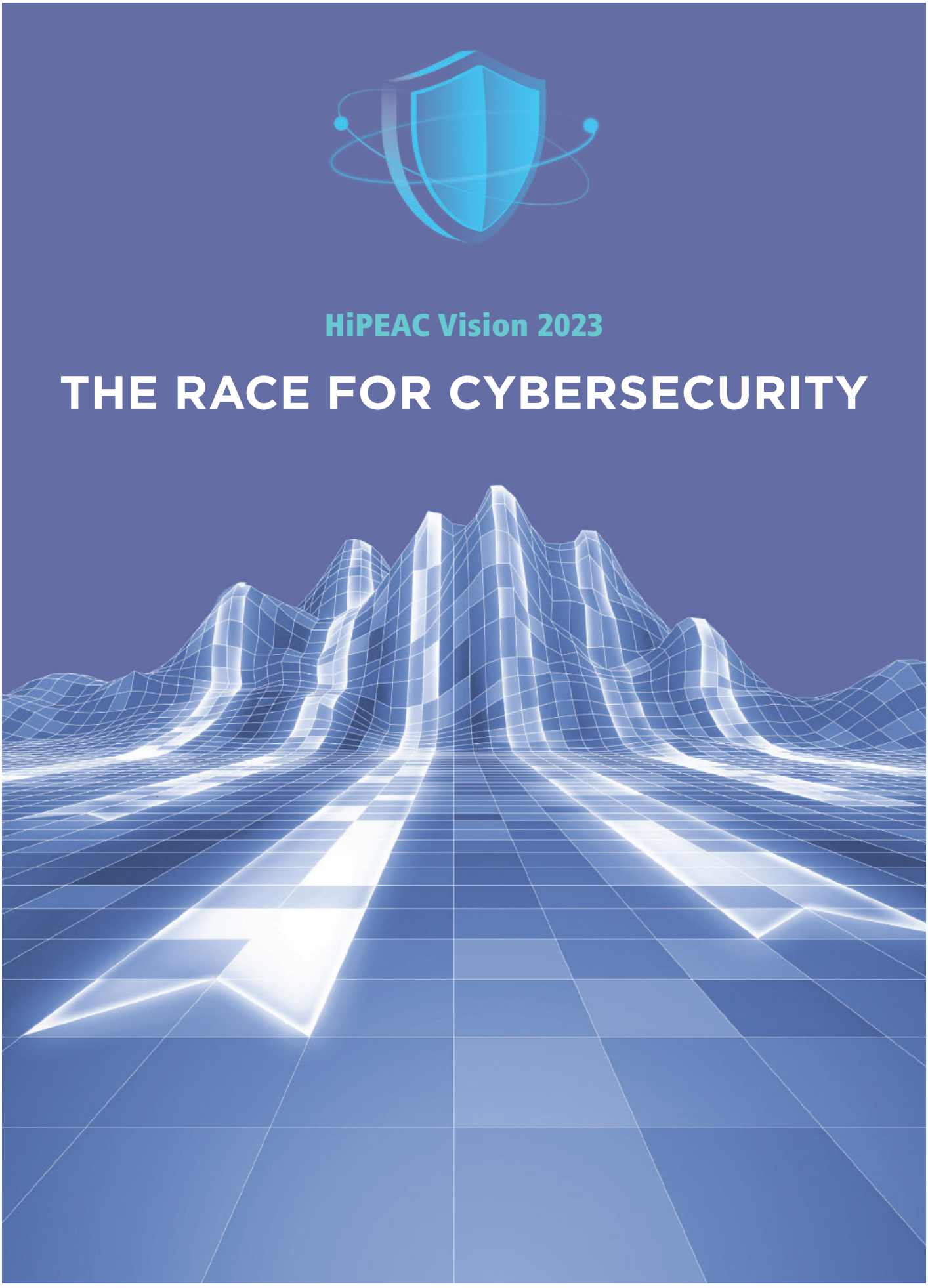
THE RACE FOR CYBERSECURITY

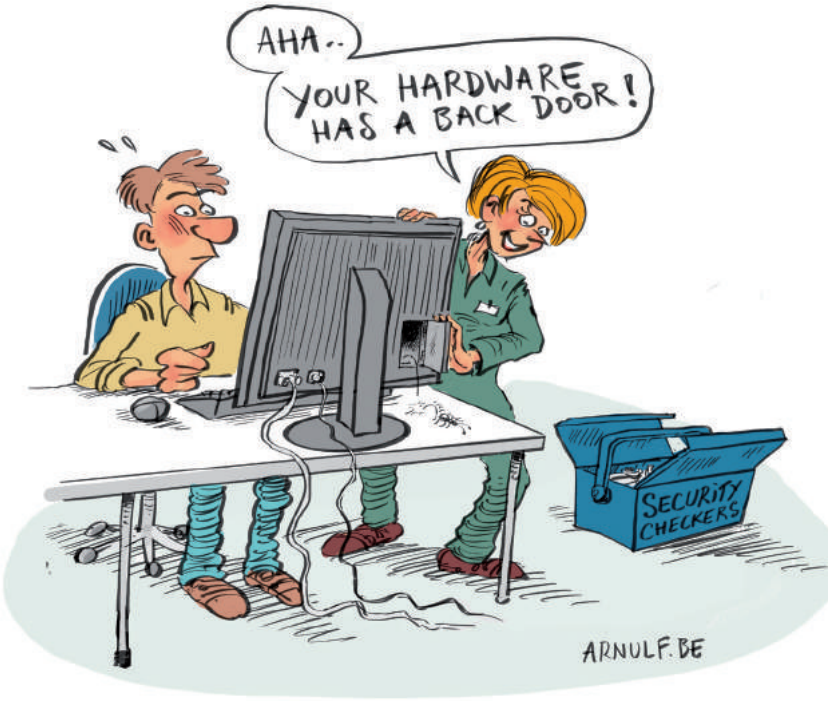
Olivier Zendra, Bart Coppens


HiPEAC Vision 2023
THE RACE FOR CYBERSECURITY

As privacy breaches, cybercrime and cyberwarfare have been soaring, significantly improved cybersecurity has both become crucial, and an opportunity for the EU to be a world leader.

The race for cybersecurity

By OLIVIER ZENDRA and BART COPPENS



After decades of digitalization spreading into every area of our lives, with very little attention given to the aspects linked to cybersecurity, information technology (IT) had essentially become an "open bar" for cybercriminals. For a few years, with a marked degradation during the peak of the COVID-19 pandemic, the news has been rife with reports of privacy breaches and cyberattacks (mainly ransomware) on companies and institutions, especially local governments and hospitals. In addition, cyberwarfare has been making the news too, especially in relation to the conflict in Ukraine.

Thus, the era of blissful ignorance and naiveté has ended. Although the wake-up call was abrupt, knowledge of these issues has expanded, and governments and to some extent businesses have taken first moves to enhance the cybersecurity frontline. However, cybersecurity is a highly competitive race between nations, between defenders and attackers, with enormous stakes. The pervasiveness of IT provides a broad attack surface, and attacks can be economically devastating, but they can also have tangible or even lethal repercussions on the physical world.

Despite several highly acclaimed advancements (e.g. the General Data Protection Regulation-GDPR), the EU still has a great deal of work to do in this regard, particularly to maintain its sovereignty and become a leader in the global competition. Cybersecurity is indeed a matter of both economic leadership and national sovereignty.

This chapter contains two contributions.

- *"From cybercrime to cyberwarfare, nobody can overlook cybersecurity any more"*
  This article describes the current state of IT system cybersecurity, showing how vulnerable systems are to the numerous dangers and challenges posed by cybercrime and cyberwarfare. It goes on to present a few concrete ways to remedy the issue, whether by technical, legal, sociological, or political means. Indeed, although the EU has weaknesses, linked to its extremely high reliance on IT systems, it also has the potential to become a world leader in cybersecurity, owing to both its strong technical culture and its regulatory capabilities.
- *"Is privacy possible in a digital world?"*
  Over the last few years, privacy has become a hot topic. However, this is in large part due to the fact that ever more data is being collected, not only by governments, but also by companies. It is often unclear for which purposes this data ends up being used; worse, it can even be leaked to third parties by attackers. Furthermore, even if this collected data would appear not to be sensitive in and of itself, sometimes sensitive information can be deduced from it. In this article, we present a summary of some of the ways in which data is gathered; how additional information can be inferred from it and how this is problematic; and how we can try to protect our privacy.

Key insights

- Ever more data is being sent to and collected from users, which has serious implications for privacy, especially when this data is analysed with big-data methods and artificial intelligence (AI).
- The scope and volume of this data is often not clear to consumers, who are sometimes even completely unaware that it is happening.
- Cyberattacks are constantly increasing, and the cost of damage caused by lack of cybersecurity is soaring. Cybercrime has become an industry, with tools and automation.
- Cyberwar has become prevalent, as shown in recent conflicts.
- The boundaries between cybercrime and cyberwarfare are blurred in some countries.
- Cyberattacks can be made at relatively low cost, and can cause very widespread and profound, even life-threatening, damage.
- There is increasing public concern for privacy and cybersecurity.
- Security and privacy must be first-class concerns of new programs from day one, in both specifications, source code and deployment. Methods and tools have to support this.
- However, legacy hasn't gone away: tools that are able to analyse the legacy code base, and find vulnerabilities and unwanted behaviour are needed, as are those that automatically circumvent or mitigate such vulnerabilities.
- Liability and certification in IT systems are crucial to the advance of security and privacy aspects. Security and privacy certification must become mandatory. Certification and liability reinforce one another. Regulation must play its role.
- Privacy and cybersecurity, hence IT sovereignty, which drastically impacts political sovereignty, depends on having control over hardware and software.
- Cybersecurity, privacy and blockchain specialists are direly needed, including for cyber warfare.

Key recommendations

- Invest in research on methods and tools to have security, including privacy, as a first-class citizen during the development of new IT systems (including e.g. quantitative security metrics/properties), find vulnerabilities in existing IT systems (e.g. with static analyses on source code and behavioral analyses at runtime), and automatically prevent or mitigate them (e.g. with automated refactoring tools and blocking system).
- Broaden mandatory security and privacy, EU-based, certification of IT systems, with several levels, and regulate to make IT systems providers and resellers liable in case of sub-par cybersecurity.
- Invest in research on automated methods and tools, possibly based on AI, for intrusion, attack and privacy breaches detection, and for active cyber defence.
- To reclaim IT sovereignty
  - base the critical parts of IT systems either on understood open-source software and hardware, or on EU-made, trustable because audited, hardware and software;
  - train more cybersecurity specialists and develop through education a culture of cybersecurity awareness in the greater workforce and public.
- Invest in post-quantum cryptography (PQC) in order to have EU-designed and EU-validated quantum-resistant encryption schemes.
- Invest in cyber warfare capacities, both for defence (resilience) and for counterstrike (deterrence).
- Harden both the hardware part and the software part of critical infrastructures and supply chains (utilities, transports, health, etc.) against cyber attacks, with reinforced cyber defences, monitoring and resilience capabilities (including redundancy).
- In addition to the above measures, harden edge and IoT devices against side-channel attacks and reverse engineering.

Olivier Zendra is a tenured computer science researcher at Inria, Rennes, France.

Bart Coppens is a part-time assistant professor and a post-doctoral researcher in the electronics department of Ghent University, Ghent, Belgium.

This document is part of the HiPEAC Vision available at hipeac.net/vision.

This is release v.1, January 2023.

Cite as: O. Zendra and B. Coppens. The race for cybersecurity. In M. Duranton et al., editors, HiPEAC Vision 2023, pages 128-129, Jan 2023.

The HiPEAC project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement number 871174.