Strategic Autonomy in The Digital World

Over 65% of the European cloud market is in the hands of US companies. There are no significant social media platforms in European hands. Although a global leader in the 1990s, Europe's share in semiconductor production has fallen to just 10% of the global market. Risk-capital investments are US dominated. These are just a few indications of how the EU is losing its strategic digital autonomy. Concurrently, our society is increasingly dependent upon a pervasive IT infrastructure, which helps preserve our most important values such as freedom of speech and democracy. This combination of factors triggered the Dutch Cybersecurity Council (CSR) to ask us to perform a novel strategic analysis of Europe's digital autonomy and cybersecurity[1], and to establish a method for developing sensible public policy[2] (**Figure 1**).
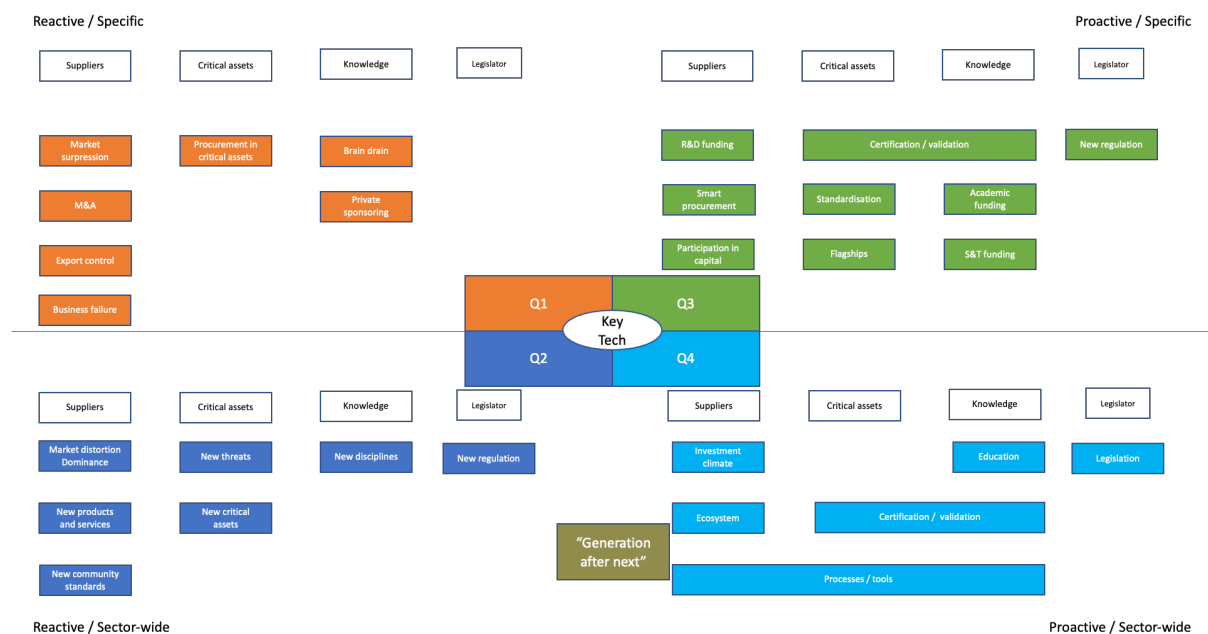

Figure 1 –Strategic assessment model to map main triggers and measures.

The study concluded that the Dutch government, together with its European partners, urgently needs to take hold of its digital strategic economy if it desires any degree of future control over the digital domain. Such 'digital sovereignty' is essential for the economy, democracy, and the stability of our society.

The guidance provided by the CSR study supports policymakers by illustrating strategic and integrated policy interventions using specific cases (e.g., cloud, secure communications, crypto) to illustrate the often-dramatic changes in control in the vast digital and cybersecurity domains. Such policy interventions can be wide ranging and could involve supporting independent scientific expertise, taking golden shares in critical companies, establishing regulatory and certification requirements for security of products and services, and becoming a launching customer of novel advanced technologies such as post-quantum cryptography.

These steps are critical because Europe has become ever more dependent on virtually uncontrollable platform and cloud providers and/or by governments attempting to spread restrictive governance and suppress human rights. With both our economic and democratic futures

---

[1] https://www.cybersecuritycouncil.nl/documents/reports/2021/02/17/report-strategic-autonomy-and-cybersecurity-in-the-netherlands
[2] https://www.cybersecuritycouncil.nl/cybersecurity-guides/documents/cybersecurity-guides/2021/11/16/guidance-on-the-use-of-the-assessment-framework-for-digital-autonomy-and-cybersecurity

threatened, we need visionary, realistic, and coherent policy, driven from the top level, to provide strategic digital autonomy.

What is "realistic" policy? First, realistic policy is *not* harking back to a glorious past, "taking back control" as per Brexit. This is not only unrealistic but also highly risky. Rather than trying to reclaim an illusory past, policy must enable control over *future* technologies, services, and products. It is also futile to dream of controlling everything as a "have it all" autarky. No sensible European policymaker lives that dream.

Realistic policy recognizes that, although Europe has important strengths and is a regulatory and economic power, it is a relative minnow in the pond of technology, defense, and investment into innovation. Realistic policy must also consider the work needed to overcome fragmentation and build Europe's "unity in diversity", as well as the sober observation that European values and norms are not globally accepted or are sometimes even rejected outright.

Thanks to AI, automated decision making is becoming pervasive throughout our society. The results can be both positive and threatening. AI brings us autonomous driving but also autonomous weapons. It can predict customer behavior but also contributes to state surveillance[3]. With machine vision also comes deep fakes. Along with improved cyberattack detection, we are faced with increasingly adaptive, automated cyberattacks.

In terms of AI, the EU's strategic autonomy situation is not much different from that of cybersecurity. Europe is no longer at the forefront of AI development due to a lack of strategic investment[4]. The US now dominates the rankings of academic institutions[5], and China is rapidly advancing. While the UK still performs top-tier academic research, major US companies (Microsoft, Nvidia, IBM, Facebook, Google, Oracle) often reap the benefits forged in Cambridge and Oxford.

Currently, very few industrial AI juggernauts exist in Europe. However, there is evidence of growing EU interest in risk investment in AI with, for example, the acquisition of Affectiva by SmartEye (SE)[6], the launch of Helsing (DE)[7] and Axelera (NL)[8], and the growth of Shift Technology (FR)[9]. Defined.ai[10], which has a very large EU-based component (PT) even though it is headquartered in the US, is another example. Key technologies in this space include AI and machine-learning algorithms/models; structured, tagged, and calibrated data lakes or data spaces; and AI-specialized chips (e.g., Nvidia/ARM, Graphcore, Tenstorrent, Axelera).

The EU should be applauded for a recently adopted strategic AI plan that coherently combines various policy activities in its approach[11]. It will be important to maintain this coherence as the action plan is executed, otherwise the plan's strategic goals will not be fulfilled.

---

[3] https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html
[4] https://www.eib.org/en/press/all/2021-181-new-eib-report-eur10-billion-investment-gap-in-artificial-intelligence-and-blockchain-technologies-is-holding-back-the-european-union
[5] https://www.natureindex.com/supplements/nature-index-2020-ai/tables/academic
[6] https://smarteye.se/smart-eye-acquires-affectiva/
[7] https://siliconcanals.com/crowdfunding/helsing-raises-102-5m/
[8] https://www.imec-int.com/en/press/dutch-ai-semiconductor-startup-axelera-ai-launches-12-million-seed-round
[9] https://www.eu-startups.com/2021/05/paris-based-shift-technology-becomes-the-latest-insurtech-unicorn-in-france-after-raising-e183-2-million/
[10] https://finance.yahoo.com/news/definedcrowd-rebrands-defined-ai-reflecting-152500874.html
[11] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence

The EU approach to AI is comprehensive in its coverage (**Figure 2**). However, we must stress that the synchronization, executional alignment, and focus of the individual actions (funding, regulation, standardization, etc.) are key to the overall impact of the approach.

Moreover, the EU plans are still very wide ranging, and it will be critical to avoid the implication that we can have it all. We must set priorities for both AI and data management. For example, the risk-based regulatory approaches planned in the AI act should be complemented by positive approaches for unlocking data. The EU can build on previous successes, such as EU Open Data[12], PSD2[13], and GDPR[14], to both unlock and protect even more data collected by public and private entities. Accessing data while keeping data protected could be facilitated through recent developments in confidential computing, which allow for data and models to be shared and used while still encrypted.

Reactive / Specific				Proactive / Specific			
Suppliers	Critical assets	Knowledge	Legislator	Suppliers	Critical assets	Knowledge	Legislator
Helsing, Axelera, Shift Technology…		Brain drain		CNECT R&D funding	Certification / validation?		EU AI act
SmartEye/Affectiva Nvidia/ARM		Private sponsoring universities		Smart procurement?	CEN-CENELEC AI focus group	AI Excellence centres	EU data act
Defined.ai				EIB AI co-investment	AI EPCIE	EU AI lighthouse	

(Center: Models / Data / Hardware)

Suppliers	Critical assets	Knowledge	Legislator	Suppliers	Critical assets	Knowledge	Legislator
FAANG NVIDIA	Surveillance	Data lakes	NIST AI RFI FTC Memo	EIB Investment support			PSD2 GDPR
Autonomous driving Digital assistants	Autonomous cyber attacks	Machine learning Machine vision		Risk investments Ecosystem			
SenseTime	Autonomous weapons	AI chips		Compare with US/CN			
		Confidential computing					

| Reactive / Sector-wide | | | | Proactive / Sector-wide |

Figure 2 – The EU approach to AI mapped to our model

We hope we have illustrated the need for strategic analysis of digital sovereignty. To achieve such sovereignty, we must be keenly aware of an evolving landscape of technologies, competitive dynamics, and geopolitics. A strategic analysis cannot be a one-off. To address strategic digital autonomy, we need a systematic, coherent, and continuous process of prospective analysis and policy development, with coordinated execution. The process must be anchored at the highest political level and should cover a wide range of policy interventions. Indeed, this is the key recommendation of the CSR study.

---

[12] https://data.europa.eu/en
[13] https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en
[14] https://ec.europa.eu/info/law/law-topic/data-protection_en