Defence companies and digital technologies

Recherches & Documents

N°02/2022

Kévin Martin
Research fellow, Fondation pour la recherche stratégique
February 2022

www.frstrategie.org

FONDATION pour la RECHERCHE STRATÉGIQUE

CONTENTS

Defence companies and digital technologies

Introduction

Companies today face the challenges brought by the growing integration of digital technologies into their production capacities and methods and their offers. Cyber security, big data, cloud computing and artificial intelligence (AI) are all technologies that are requiring them to rethink their business model, in all business sectors. This digital transformation can lead to radical changes in the way they organise work and manage innovation (products and technologies) and significantly affect their business opportunities, in particular. These changes also concern the business environment, with the redefinition of value chains and ecosystems and the advent of new competitors with different profiles. Historical defence companies do not escape these fundamental trends.

The national defence strategies of major powers all concur on the growing role and use of these technologies for and by their armed forces. Mastering digital technology is regarded as a matter of sovereignty. In recent years, dedicated national strategies have thus been defined for cyber security and AI. However, in these fields, defence companies find themselves facing competition from predominantly commercial companies, active in the development of web and IT services and hardware production.

This note aims to explore the various stakes involved for defence companies in developing and maintaining digital business (cyber security and AI), in a context of fierce competition.

1. Specific features of digital solutions markets

1.1. Diverse and dynamic markets

Digital offers cover a wide variety of solutions in all fields of technology, thereby rendering these markets very difficult to analyse. In cyber security for example, solutions can be distinguished according to the type of offer (hardware, software, related services) or the security functions required. Through its annual observatory, France's *Alliance pour la confiance numérique* (Alliance for Digital Trust - ACN) segments the market into digital security solutions on the one hand, and cyber security products and services on the other. However, for each of these solutions, the market dynamics can prove to be very different.

Figure no. 1: SCOPE OF DIGITAL TRUST, SEGMENTATION OF SOLUTIONS

<table>
<tr><th rowspan="2">Digital Security</th><th colspan="2">Cyber Security</th></tr>
<tr><th>Products / Software</th><th>Services</th></tr>
<tr><td>Access control</td><td>Cyber Governance
Management systems / SEM</td><td rowspan="2">Cyber Auditing, Planning and Consulting

Vulnerability testing / Risk evaluation, Information security audit / Risk and threat analysis and management / Security strategy consulting, planning and management / Security certification, compliance assessment, IT security evaluation / Forensics, investigation and analysis</td></tr>
<tr><td>Individual Identification & Authentication
Biometrics / Smart cards / Badges, ID cards, etc. / Vehicle recognition / Anti-counterfeiting</td><td>Identity and Access Management</td></tr>
<tr><td>Large Area Observation
Optronic systems / Radar / Satellite imaging</td><td>Data Security
Encryption, cryptography, digital signature / Public Key Infrastructure / Digital rights management / Content filtering and anti-spam / Secure archiving</td><td>Cyber Implementation
Project management, modelling, engineering and architecture / Integration, implementation and testing / Project support</td></tr>
<tr><td>Tracking and Locating
Tagging and tracking (RFID, barcode, Wi-Fi, etc.) / AIS, LRIT systems, etc. / Electronic seals with tracking and positioning (GPS, RFID)</td><td>Applications Security
Software development / Secure OS / Bug bounty platforms</td><td rowspan="2">Securing facilities management and operations
Operating support / Managed security services, cyber security service operations management / Facilities management security / Continuity management and recovery / Trusted third parties and content and reputation management services</td></tr>
<tr><td>Control Command Decision Aid
Information and decision management / simulations / other</td><td>Digital Infrastructure Security
Firewalls / antivirus / anti-DDoS / intrusion detection / Cyberthreat / Communications security: phone, videoconferencing and messaging / Secure remote working platforms / Trusted Cloud / Blockchain</td></tr>
<tr><td>Intelligence Information Collection
Interception / Tapping / Locating / Big data / Investigation</td><td>Product and Equipment Security
HSM / Secure elements</td><td>Cyber Training</td></tr>
</table>

Source: ACN, *Observatoire pour la confiance numérique,* 2021

In artificial intelligence, the segmentation appears to be just as problematic[1]. As commercial rollout of AI is still in its early stages, most AI solutions are specialised products for specific areas, and the market currently resembles a fragmented set of technological building blocks, be it in natural language, vision or speech processing, or autonomy in robotics.

[1] Olivier Ezratty, *Les usages de l'intelligence artificielle*, Creative Commons, Edition 2021, 742 p.

Figure no. 2: FUNCTIONAL APPLICATIONS OF AI: AN EXAMPLE OF SEGMENTATION

Source: *WIPO Technology Trends 2019: Artificial Intelligence*[2]

Depending on the technological building blocks, industrial (and commercial) developments are at very different levels of maturity. The main solutions sold therefore focus on machine learning technologies with different approaches (supervised or deep learning in particular). However, AI encompasses many sub-categories of technology which do not use data in the same way, in terms of volume and quality. Thus, the wealth of the very concept of artificial intelligence does not truly emerge in the current industrial landscape, especially since work has focused on connectionist AI technologies[3].

As regards hardware, processors and microprocessors are the centre of attention due, especially, to the boom in AI technologies relating to machine learning. These solutions largely depend on the development of storage and computing capacities. Once again, market dynamics emerge depending on the type of architecture (GPGPU, neuromorphic processors) or the infrastructure to be equipped (cloud server, sensor/effector).

In general, these fields of technology have no shared definition and cover an array of technological families whose possibilities are explored simultaneously and are at very different stages in their development. Market analyses and growth prospects therefore

[2] WIPO, *WIPO Technology Trends 2019: Artificial Intelligence*, 2019.

[3] AI comprises two main technical branches, connectionist and symbolic AI. As the report drafted by the Ministry of the Armed Forces' AI Task Force indicates (Stratégie de l'Intelligence artificielle au service de la Défense, 2019), "*symbolic approaches* [are] *based on reasoning (rule-based systems) and connectionist approaches, which are closer to empiricism, on learning from large databases (networks of neurons)*".

depend heavily on the scopes taken into account. While they are often presented as disruptive solutions allowing new methods or uses to be developed (and bringing new security needs), these fields of technology are characterised by extremely rapid innovation cycles.

1.2. A fragmented and highly segmented demand

For all these digital technology markets, demand is also very disparate and is segmented according to geographical location, customer type and even the sector of business.

The US market would appear to be crucial for solution providers, whatever the field. For example, in cyber security, it accounted for almost 37% of global demand in 2019[4], according to the European Cybersecurity Organisation (ECSO), thereby giving US firms a competitive edge due to a "major market effect". European markets (excluding the UK) represent a 13% share. But this figure is aggregated. The EU is still a very fragmented market, which compels companies to adopt national approaches, despite initiatives aiming to consolidate it (NIS Directive, Cybersecurity Act)[5].

Four main market types can also be identified based on the profile of their end customers, which are characterised by a number of determining factors such as the required standard of security, functions and budget. With this breakdown into four main categories, the analysis can be adjusted to the requirements and specific features of each customer profile (size, market maturity and particular needs), but it is not set in stone. Some common characteristics can emerge.

- **Defence**

  This market is regarded as very mature (except for innovation niches), requiring the most complex technologies with solutions that are generally produced and marketed by defence industry firms. Demands are higher in terms of security, compliance and data privacy as these solutions are often linked to areas of sovereignty. While contracts are often signed for high amounts, they are awarded in small numbers (multi-year contracts) and generally concern small series. Access to this type of market is therefore limited and it regularly sees mergers between industrial players of varying sizes in order to meet the complex technical needs.

[4] Carlos Alberto Silva, "The current status of private investment in cybersecurity and effort until now at European level", ECSO Presentation at the 9th Cyber Investor Days, 15 June 2021.

[5] Passed by the European Parliament in 2016, the NIS Directive particularly aims to define a series of shared requirements applicable to information and network security for companies designated as operators of essential services (OES). The Cybersecurity Act, a regulation adopted in June 2019, goes further by giving ENISA (the European Union Agency for Cyber Security) a permanent mandate and defining, for the very first time, a European cyber security certification framework. However, as the French Information Systems Security Agency ANSSI states, "*It shall be noted that in itself, the Cybersecurity Act defines a framework and governance but without specifying the rules for certification. Products, services and processes destined to be certified will be successively covered by thematic schemes.*" Cf. ANSSI, *Papiers numériques*, September 2021.

- **Governments**

  This market has security and compliance requirements that, in some respects, are similar to those of the Defence market. For cyber security, cloud computing or AI solutions, needs may particularly be overseen by public authorities (like the French Agency ANSSI) and must meet predefined standards. This market has the particular feature of requiring certification for cyber security and, henceforth, cloud computing products and solutions. The cost of obtaining certification can be a barrier for certain companies and access to this market is therefore challenging.

- **Large enterprises**

  Requirements are determined individually by customers based on their needs and expectations (subject to any sector-specific or particular regulations, such as for operators of vital importance (OIV). The geographical dispersal of production, management, supervision and industrial sites as well as growing international competition are prompting major companies (and mid-caps) to look for innovative solutions offering a good price-performance ratio, in the context of their digital transformation. These are highly profitable but also very competitive markets.

- **Retail / SMEs**

  This market is geared towards “general public” needs, i.e., turnkey solutions with low cyber security requirements. Budgets are generally quite small and the solutions are almost always comprehensive offers. Given the complexity of the market, “private” customers give priority to buying market-leading solutions from recognised companies.

In addition to being industrial players, integrators (mainly consulting and digital service companies) are also a customer category as they act as intermediaries in a high number of large-volume contracts.

Lastly, civil markets must also be examined from a business angle in order to assess the different market dynamics. A great many digital solutions take the customer’s specific requirements into account depending on their sector of activity (such as retail trade, banking/finance, health or logistics). As the preferred selling method is B2B, providers adapt their solutions to their customers’ specific context, legal rules and technical standards, which renders economies of scale more difficult to achieve.

2. An industrial environment marked by the leading position of digital players

National capacities in digital technologies have generally developed thanks to the prior existence of the hardware industry (PC and components, calculators, electronic boards and chips, semi-conductors), and defence, telecommunications, software and consulting industries. In the case of artificial intelligence, players historically positioned as web service

providers (Google, Amazon, Facebook) are today among the leaders in the field after adapting their original offering and leveraging the masses of data they possess.

In addition, scattered demand and the specificities of digital technologies – AI and cyber security for example – explain why industrial players pursuing predominantly civil activities are omnipresent.

2.1. Strategies and profiles

2.1.1. The vertical integration strategy of the major digital players

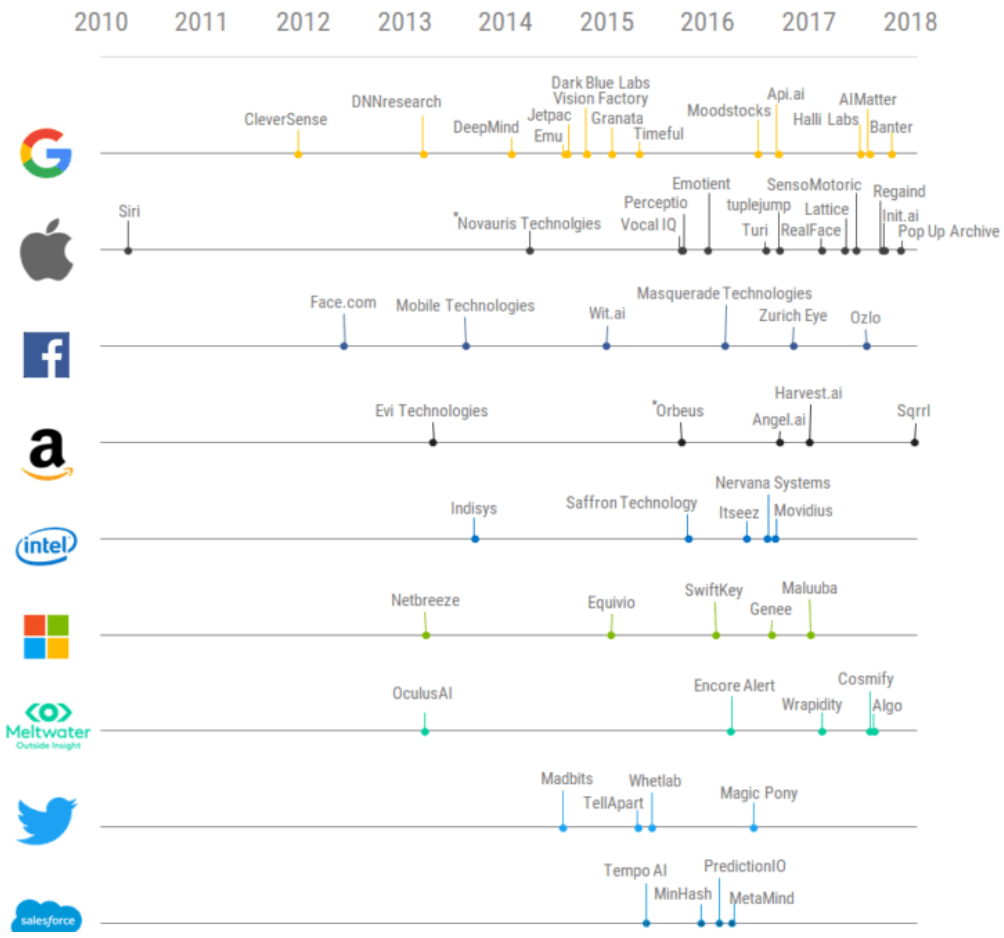
In the past, the main players in digital technology such as IBM (founded in 1911), Intel (1968), Microsoft (1976) and Apple (1976) came from the IT world (hardware and equipment manufacturing, operating system development). They are almost exclusively American and have sought to diversify their businesses in order to reduce their exposure to the hardware market (which has been marked by a downward trend in demand and competition from emerging players, especially Chinese).

They have all opted for a vertical integration strategy through an asset acquisition policy, primarily targeting software publishers and IT service providers. Today, they offer complete solutions, reflecting the shift from a sales model based on IT products and services[6]. By means of dynamic external growth, these players base their expertise on their ability to keep up with technological developments and new uses impacting their markets (products and customers). In the years 2000, these organisations therefore positioned themselves as data managers and digital service providers, and shed their historical hardware manufacturing business where necessary[7]. In this sense, their strategy is similar to the one deployed by companies such as Amazon, Google and Facebook. They have integrated cyber security solutions into their traditional offering but without actually being positioned in this market *per se*. However, AI would seem to be a natural shift in their core business, not to say a vital move to retain their position in the value chain as key players in the digital transformation of organisations.

[6] E.g., switch from Office Suite to Office 365 at Microsoft.

[7] For example, in 2005, IBM sold its PC operations to Lenovo. In 2014, the Group spun off its x86 server business (to Lenovo) and a part of its historical production of ex-PowerPC chip-type semi-conductors for Apple, Xbox, etc. (to Global Foundries).

Figure no. 3: EXAMPLE OF ACQUISITIONS OF AI START-UPS BY DIFFERENT US GROUPS



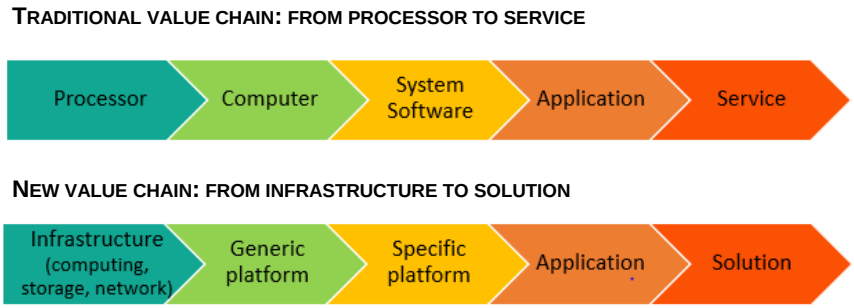
Source: CB Insight

In this context, the main strategy pursued seems to be the development of multi-platform or multi-field management systems based on technologies using machine learning. By offering these fundamental building blocks, they can integrate numerous specific solutions adapted to each sector or customer.

Microsoft, for example, has radically changed its strategy, as illustrated by the predominance of its "Azure AI" cloud computing offer in which AI plays a core role. Azure AI is more specifically based on the firm's hosting capacities – and on the data it holds – to offer an AI Platform-as-a-Service (PaaS) capable of hosting various open source or other libraries such as TensorFlow[8], as well as software applications developed in-house. The aim is to position the company as a core network of businesses/institutions in artificial intelligence with multiple applications. Microsoft's system is therefore semi-closed, with the ambition of aggregating applications developed outside the company on a proprietary cloud platform.

[8] Open-source machine learning tool developed by Google.

Figure no. 4: CHANGE IN THE IT VALUE CHAIN



Source: Gérard Roucairol, Pierre Bitard, "Pour une politique industrielle du numérique", *Les cahiers Futuris*, March 2018, pp. 31-33

Furthermore, key digital players have published open source basic AI software components providing numerous start-ups, SMEs and even large companies with a framework for developing business solutions (TensorFlow in particular). They *"adopt a twofold approach based on platforms to appeal to app developers with mostly open source frameworks and generate economies of scale, and vertical integration to capture an equally large part of the added value"*[9]. This results in a misleadingly open architecture where the end-to-end control of the chain leads, in practice, to a sort of ecosystem in the hands of a single player[10].

These key players also have R&D capabilities enabling them to retain or create processor development activities (specific to AI applications). In this segment, their industrial strategy is similar to that of pure-play equipment manufacturers (via vertical integration).

2.1.2. Software publishers at the heart of digital innovation

Software publishers represent the largest group of players. While the world leaders are large, pure-play companies, historically positioned in the cyber security market, generally non-European and listed on the stock market, this category also includes a myriad of start-ups and SMEs. Today, all attentions are on the latter thanks to their offensive marketing and communication strategy. They are often highly specialised in a given sector (finance, health, e-commerce for example) and/or an application (voice recognition/speech processing, computer vision, data mining, optimisation, AI calculators, etc.).

Start-ups and SMEs are traditionally regarded as the most innovative firms. They develop partnerships with other types of companies or are the target of acquisitions. However, most of these firms, and especially those positioned in application segments, adopt a specific approach to the market. In this case, software publishers integrate numerous software components and computing capacities available off the shelf and developed/managed by leading digital groups.

[9] Olivier Ezratty, *Les usages de l'intelligence artificielle*, ebook Blog Opinions Libres, October 2017, Chapter "Acteurs de l'intelligence artificielle", p. 242.

[10] For instance, Google/Alphabet which markets the TPU, services around TensorFlow and its numerous databanks.

For these players, customer confidence is a major issue, i.e., their confidence in the company's ability to implement a large-scale solution or drive a sustainable industrial strategy, etc. In the start-up or SME stage, the crucial aim for software publishers is to have sufficient funding capacities to ensure their growth phase. This stage is crucial to win a dominating position in an economy marked by hyper-growth. However, doing several funding rounds can cut two ways[11]. Although it can be an indicator of a start-up's attractiveness – and of the potential for its solutions and/or innovations to access the market – it can also lead to a loss of control (capital dilution) and a shift in the company's strategy.

The different stages in capital requirement of innovating start-ups

In general, a start-up's capital requirements break down into five stages according to the maturity of the project:

- **Project design**. At this stage, funding is usually provided by the founders. As an example, requirements are between €50K and €100K for a European cyber-security start-up.
- **Seed**: in this stage, a legal corporate structure is created. In general, seed funds are between €100K and €500K and are intended to support the start-up through its industrialisation/marketing phase.
- **Early-stage** is when the start-up begins to have customers and generate revenue. The funding rounds, called Series A and Series B, reach €0.5 million to €5 million on average. Setting up an experienced management team plays a key role in attracting venture capital funds.
- **Late-stage** is the point at which the start-up has proven that its project is viable through strong commercial presence. Funding rounds are therefore higher (more than €5 million).
- **IPO**. To reach this stage, the company must first reach a critical size before seeking to make a profit. Late-stage funding allows the start-up to invest in marketing and R&D to attain it.

Among publishers specialising in AI, the case of the American firm Palantir, which generated revenue of €1.1 billion in 2020, is worthy of note. Positioned in the structured and unstructured data mining and analysis segment, the company offers two software solutions. The first, "Gotham", is its historical solution targeting customers in Defence and intelligence; it accounts for 56% of its business. The second, "Foundry" (44% of revenue in 2020), is more specifically intended for civil markets. Founded in 2004, Palantir completed its initial public offering in 2020. The US publisher's emergence and growth are based on several factors, including its management team's strong experience in entrepreneurship and digital technology and its close relationship with the US intelligence community (influence of the IN-Q-TEL fund, access to specialised HR, commercial opportunities). Its commercial offer was also one of the frontrunners in this segment (with the British firm i2 in particular) and Palantir has regularly carried out substantial funding rounds (totalling $2.6 billion[12]) that have played an important role in its growth by supporting marketing and R&D activities and

[11] Presentation of Nextflow at the conference organised by Atlanpole, "Peut-on développer sa start-up sans lever des fonds ?", 14 June 2016.

[12] "Palantir Technologies", *Crunchbase*, consulted on 8 September 2021.

buyouts of strategic assets. Palantir has effectively bought out several companies whose capacities have reinforced the firm's specialised teams (Voicegem in 2013[13]) and brought additional technological building blocks. This is the case of the transactions carried out between 2014 and 2016 targeting Propeller (app-making), Poptip (real-time social media data analysis), Silk (data display) and Kimo-no Labs (web-scraping tools). Palantir also signed a settlement agreement in 2011 with the British firm i2 following a lawsuit brought by the latter for infringement of intellectual property[14].

For European start-ups, particularly those specialising in AI or cyber security, access to private venture capital funding is regularly regarded as a stumbling block, particularly in the last stages of a project (Late Stage and IPO)[15]. Exit is indeed a crucial issue for start-ups. As a reminder, it can take place in three ways:

- Buyout of the start-up by a large company in the sector;
- Acquisition of stakes by private equity and specialised investment funds;
- IPO.

The first would appear to be the preferred option in Europe. Conversely, there are still few examples of IPOs or French/European funds positioned in financing the late-stage growth of start-ups. This is a well-known obstacle to the development of this industrial ecosystem but is increasingly a focus point of national and European public policies.

2.1.3. Digital service companies: what place in the value chain?

Service providers involved in AI are mainly global digital service companies. They take advantage of their "key account" customer references to roll out solutions within information systems. One of the main challenges for global digital service companies is their ability to develop a trusting and close relationship with end customers. To do so, they must provide a nationwide network, partly by setting up service sites linked to the group. Abroad, where they face similar issues, major digital service companies favour a multi-domestic strategy in order to be sufficiently close to the end customer. In this context, these firms can operate as integrators. Some are active in AI to strengthen their digital transformation offering for their long-standing customers (public and private key accounts), and they multiply their acquisitions and partnerships with key digital companies and software publishers.

[13] "Palantir Acquires Team Behind YC Voice Email Startup Voicegem", *Techcrunch*, 16 February 2013.

[14] "Palantir's third black eye: i2 lawsuit settled", Reuters, 17 February 2011. i2 was taken over in August 2011 by the American firm IBM.

[15] "Web conférence : Financement et développement des startups évoluant dans le domaine de la défense", Fondation pour la recherche stratégique, 9 July 2020.

2.2. New strong competitors in the defence markets?

Major global companies that have developed through the various waves of IT and digital technology (IBM, Microsoft, Apple, Amazon, Google and Facebook) are today the key players in digital technology.

They are characterised by:

- a very large and varied customer base in the civil market;
- positioning in highly profitable businesses and markets (integration, consulting and related services);
- considerable investments in R&D;
- for the largest ones, sufficient cash flow to pursue ambitious acquisition policies targeting strategic assets.

Alongside them, a great many specialised firms have developed a service offering to be positioned on a part of the value chain. Therefore, in addition to dynamic external growth, key digital firms also drive a dedicated policy of partnerships with start-ups and SMEs (e.g. business incubators or collaborative labs). As their internal organisations are considered too cumbersome to deliver the short cycle required in innovation, major companies need to cooperate with more innovative and agile organisations. In this context, "*digital natives have also been forerunners in the creation or implementation of partnerships with entities such as business incubators, accelerators (…). They therefore maintain their ability to explore fields related to their core business, and foster regular competition with their in-house R&D teams*"[16]. Start-ups and SMEs are therefore fully integrated into the ecosystem of these major organisations. And while key digital firms partner with start-ups and SMEs in R&D (by creating appropriate innovation systems such as innovation centres or labs, often abroad), they are also customers and integrators of the solutions these companies develop, and even investors via specialised and recognised corporate venture funds.

The reconfiguration of the IT value chain stemming from changes in digital technology is leading specialised digital firms (leading groups, software publishers and digital service companies) to capture an ever-increasing share of the added value generated by businesses operating in "traditional" sectors. In some cases, they compete with historical industries in their core business by adopting a "digitally native" organisation. The cases of SpaceX in space launchers and Tesla in the automotive industry are a perfect illustration.

Telecommunications operators also face this new competition[17]. While they primarily buy off-the-shelf solutions, particularly in the context of their customer relationship (such as chatbots and voice recognition services) or predictive maintenance and network optimisation, telecom operators could see their business model evolve, especially with the central role taken by cloud computing services (and infrastructure) and the deployment of the 5G network (related business opportunities in the field of smart objects).

[16] Sébastien Tran, "Comment les digital natives sont-elles devenues les entreprises les plus innovantes du monde", *The Conversation*, 10 April 2018.

[17] "Comment les GAFA s'invitent sur le terrain des télécoms", *Le Monde*, 27 September 2021.

The Defence industry is not escaping these trends. Some civil digital firms are clearly setting out to penetrate the Defence market and succeeding in winning major contracts. Palantir is now one of the main suppliers of the DoD, rivalling with historical players. In March 2019, the firm was selected for the US Army's modernisation programme – Distributed Common Ground System (DCGS-A) – over Raytheon (contract assessed at $800 million)[18]. In 2021, Palantir won phase 2 of this programme over BAE Systems ($823 million)[19]. And although they were cancelled in July and October 2021, the Joint Enterprise Defense Infrastructure – JEDI contract (for which Amazon and Microsoft competed) and Integrated Visual Augmentation System – IVAS contract (won by Microsoft), respectively worth $10 billion[20] and $21.9 billion[21], are a further reminder that key digital players have become vital for the armed forces.

In France, digital service companies are showing growing interest in the Defence market. Both Atos and Sopra-Steria are involved to varying degrees in the Artemis programme of the French Armed Forces Ministry. Atos, which is positioned in Defence partly as a result of acquiring the historical businesses of Bull[22], has founded a joint venture with Thales[23].

These developments are revealing new issues for Defence customers. The case of the MAVEN project involving Google and the DoD, relating to the use of shape recognition algorithms in US armed drone targeting, is a good example. The project's media coverage and then its discontinuance by Google under pressure from the company's engineers, reflect internal tensions arising around the development of solutions for the military world[24]. Other difficulties inherent in the Defence market also limit its appeal, including exclusively national demand, solution compliance and security, and the need for differentiation.

3. Defence companies: customers, digital solution providers and partners

The integration and command of new, digital technology building blocks have become key challenges for defence companies. They are vital in the context of the internal digital transformation plans initiated in recent years with the aim, in particular, of modernising

[18] "Palantir – who successfully sued the Army – has won a major Army contract", *Defense News,* 29 March 2019.

[19] "Palantir captures another Army battlefield intell system award", *Washington Technology*, 6 October 2021.

[20] "Le Pentagone ouvre à la concurrence le contrat cloud JEDI remporté par Microsoft contre Amazon", *L'Usine digitale*, 7 July 2021.

[21] "U.S. Army pushes back date on Microsoft goggles, affirms commitment to deal", Reuters, 14 October 2021.

[22] In May 2014, Atos announced a take-over bid on Bull, valuing the firm at €620 million. This deal allows the group to extend its operations to the production of IT equipment and hardware (HSM, hard drives, HPC, etc.), a part of which is dedicated to Defence, while expanding its offering in cloud infrastructure and consolidating its position in artificial intelligence.

[23] "Thales et Atos officialisent la création d'Athea, 'champion' de l'intelligence artificielle pour la Défense", *Opex360*, 27 May 2021.

[24] "Google Hedges on Promise to End Controversial Involvement in Military Drone Contract", *The Intercept*, 1 March 2019. This has not prevented Google from having several contracts with the DoD: "Forget project Maven. Here are a couple other DoD projects Google is working on", *C4ISRnet*, 13 March 2019.

industrial facilities. But they are also vital to respond to the new needs of their traditional customers and, as the case may be, their change of positioning (dual-use activities). Defence companies are therefore both customers and potential providers of digital solutions.

3.1. The various ways of integrating digital technologies

In the case of defence activities, and due to requirements specific to public authorities, various challenges can be identified according to the degree of integration of digital solutions:

- Generic digital solutions available in the civil market and which can help to improve a defence company's productivity;
- Digital solutions adapted to Defence needs;
- Digital solutions designed specifically for Defence purposes and integrated into arms programmes.

AI: the challenge of managing and using data for defence companies

Dominant players in artificial intelligence (e.g. AWS, Google and Facebook) have developed sound expertise, often by capitalising on their ability to access huge amounts of different data. The management and processing of these data therefore give them a decisive advantage in view of the current types of AI available on the market, based on machine learning.

In the field of defence, data management involves several issues, namely: access (confidence of the public authorities in sharing them); management and storage (protection of classified data); and volume ("small series" effects of weapons systems deployed).

As a customer or partner, the strategic choices made by companies focus primarily on organisational, management and HR aspects and on the integration of off-the-shelf solutions into their industrial facilities. The actions taken can be summed up as follows:

- Identification and evaluation of opportunities to create value with data available in the company and introduction of new governance for data (improving access by de-siloing different data sources within the entity and securing digital assets).
- Integration of off-the-shelf solutions, i.e. adopting solutions designed above all to improve/protect the business, mainly support functions (company infrastructure, HR, purchases, R&D) and basic functions (logistics, manufacturing/production, distribution, sales/marketing and services).

Defence companies thus implement solutions provided by partners or suppliers and adapt them to their own needs and requirements. They also have to deal increasingly with onboarding staff that are specialised in these new technologies. This is another major challenge given the shortage of labour and heightened competition with key players and other predominantly commercial organisations.

Beyond internal uses, the actions taken by defence companies aim to adapt or complete their catalogue of solutions, with the risk of undermining their position in the value chain or

even being ousted from big new defence markets (partly relating to the shift from information and communication systems to cloud-based architectures). In this context, defence companies may need to develop specific new solutions by focusing on R&D. They may also wish to secure a position in other markets (business or customer diversification) by buying out specialised firms (external growth policy), and/or adopt an approach aiming to share risks and financing efforts by signing agreements with other players, whether or not specialised (partnership policy).

The cyber security strategies carried out by defence companies in the US and Europe in the years 2010 provide some first feedback on the challenges inherent in moving into these new fields. The most recent strategies implemented in AI and big data in particular suggest a preference for a partnership approach, with the dual aim of consolidating an ecosystem of innovative entities around defence companies and integrating "civil" mechanisms relating to the development of digital technologies.

3.2. Digital solutions providers: feedback from cyber security markets

Defence industry players gradually moved into digital markets in the mid-2000s with cyber security. Identified as a potential growth driver, at a time when orders for defence equipment were shrinking, the cyber security market saw defence suppliers such as Raytheon, Lockheed Martin, Northrop Grumman, General Dynamics, BAE Systems, Airbus Defence & Space, Thales, Safran, Leonardo and Rohde & Schwarz arrive in force. This penetration was achieved essentially through external growth strategies, with the aim of expanding their portfolios of products/services (new specific markets) and customers (private players and governments)[25]. However, by broadening their offer so as to reach the civil market, defence companies found themselves in direct competition with historical digital companies (key digital players, specialised software publishers and digital service companies). They also found themselves in a market with a very different business model to their traditional activities which demands significant venture-capital investments.

3.2.1. In the US: the gradual withdrawal of defence companies from cyber markets

In this context, after setting up specialised subsidiaries or business units (following a series of buyouts), most US defence companies then made a U-turn, and sold them off.

[25] Kévin Martin, "Cybersécurité : ambitions israéliennes et positionnement des acteurs défense", *Défense & Industries,* No. 6, February 2016

Figure no. 5: ACQUISITIONS / SALES OF CYBER AND IT BUSINESSES BY THE MAIN US DEFENCE COMPANIES

	Main cyber and related business acquisitions	Sales of cyber and IT businesses
Lockheed Martin	Eagle Group International LLC (2009), Amor Group (2013), Industrial Defender (2014),	IT & Technical Services businesses (2016)
General Dynamics	Vangent (2011), Fortress Technologies (2011), Fidelis Security (2012), Open Kernel Labs (2012), CSRA (2018)	Fidelis Security (2015)
Boeing	Narus (2010), SMSi (2011), Inmedius (2012), Ventura Solutions (2014)	Narus (2015)
Northrop Grumman	M5 Network Security (2012)	IT & Missions Support Services businesses (2021)
Raytheon	Oakley Networks (2007), SI Government Solutions (2008), Telemus Solutions (2008), BBN Technologies (2009), Compucat Research (2010), Technology Associates (2010), Trusted Computer Solutions (2010), Applied Signal Technology (2011), Pikewerks Corporation (2011), Hengeller Computer Consultant (2011), Teligny (2012), Blackbird Technologies (2014), Websense (2015), Stonesoft (2016), Sidewinder (2016), RedOwl (2017), Skyfence Network (2017)	Forcepoint (2020)

For example, in 2016 Lockheed Martin sold its IT & Technical Services businesses to Leidos, thereby withdrawing from government contracts. However, the US group retained its most critical cyber operations. Dan Nelson, VP Corporate Communication, summed up the reasons for this sale as follows: "*The main factors driving the spin-off or sale of our IT and technical services businesses (which include cybersecurity) are changing market dynamics, shifting government priorities, increased competition and industry trends that have led us to believe that these businesses may achieve greater growth, and create more value for our customers by operating outside of Lockheed Martin*"[26]. The situation is similar for Boeing with the sale of its subsidiary Narus, five years after its acquisition. More recently, Northrop Grumman and Raytheon have sold off their IT or cyber businesses (IT & Mission Support Services entity for Northrop Grumman, and cyber security subsidiary Forcepoint for Raytheon).

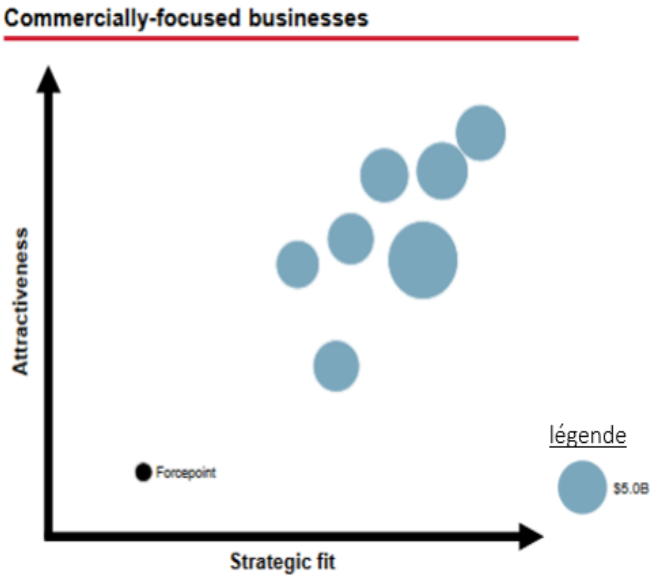
Prior to its merger with UTC, Raytheon was one of the few historical US defence groups to conduct a diversification strategy to civil cyber security markets. The group bolstered its existing solutions offering with cyber capacities (missiles, radar, ISR, C2, etc.) while diversifying its business for digital transformation markets (threat detection and management in particular). To do so, Raytheon pursued a sustained external growth policy between 2007 and 2016 with 15 acquisitions totalling more than $3.5 billion. The main transactions included the buyout of a pioneer in IT, BBN Technologies (2009), a defence and intelligence specialist, Blackbird Technologies (2014), and a firm active in civil markets, Websense (2015). Initially, this policy led to a consolidation of cyber security operations within a dedicated division called Raytheon Cyber Products. Then, in May 2015, with the purchase of Websense, Raytheon moved to a new level by consolidating all of the group's

[26] "Lockheed Martin Corp. To Exit Commercial Cybersecurity, Double-Down on Helicopters And Combat Jets", *Forbes*, 4 December 2015.

civil market offers in a cyber security subsidiary (merging the assets of Raytheon Cyber Products with those of Websense in Forcepoint).

The sale of its commercial cyber security subsidiary Forcepoint was nonetheless a possibility put forward in 2018-2019. The group's 2018 Annual Report already stated that: "*In order to compete effectively, Forcepoint must successfully execute on its growth strategy, including the development of new products and services. If Forcepoint is unable to compete successfully, it may divert financial and management resources that would otherwise benefit our other operations*". The sale finally took place in January 2021 as it was no longer worthwhile making the necessary investments due, in particular, to the high operating costs generated by sales and marketing (43% of 2019 revenue). The cyber subsidiary's results were also already well below the other businesses and therefore detrimental to the group's performances; Forcepoint's operating margin was barely 1.2% in 2019 compared to an average 16.4% for the group[27]. However, Forcepoint's operations were marginal and accounted for only 2.25% of the group's total revenues ($658 million).

Figure no. 6: VALUATION OF RAYTHEON TECHNOLOGIES' COMMERCIAL PORTFOLIO



Source: Raytheon Technologies Investor Day[28]

The sale of Forcepoint was also an indication that Raytheon had integrated all the cyber-security technologies into its core business and diversified the profile of its teams (side effect). In addition, it reflected a repositioning in digital markets (need to concentrate investments) at the time of the Raytheon-UTC merger. After announcing in 2018 that its R&D centre BBN Technologies had been selected by DARPA as part of the Explainable Artificial Intelligence programme (XAI), the group signed a strategic agreement with IBM in 2021 for the joint development of AI and quantum technologies.

[27] Raytheon 2020 Annual Report.

[28] Greg Hayes (CEO Raytheon Technologies), "Raytheon Technologies Investor Day", 27 July 2021.

Meanwhile, General Dynamics appears to have retained a dual approach to its cyber and IT businesses, and is the only US defence supplier to follow this course. The acquisition of CSRA in late 2018 for $9.7 billion confirms this trend[29]. More generally, despite the divestments from civil markets, all the players have retained cyber expertise and offers designed for Defence customers or directly integrated into their historical offerings.

3.2.2. In Europe: the consolidated presence of defence companies on cyber markets

In Europe, with the 2016 sale of its subsidiary Morpho to Oberthur, only the Safran group opted to refocus on its core business in aerospace and defence. Conversely, the other European defence companies have chosen to structure capacities on several segments and have gradually become key players within national industrial and technological cyber security bases[30].

Figure no. 7: ACQUISITIONS / SALES OF CYBER AND IT BUSINESSES BY THE MAIN EUROPEAN DEFENCE COMPANIES

	Main cyber and related business acquisitions	Sales of cyber and IT businesses
Safran	L-1 Identity (2011), Dictao (2014)	Morpho (2016)
Thales	Sysgo (2012), Alcatel-Lucent cyber businesses (2014), Vormetric (2015), Guavus (2017), Gemalto (2019), Ercom (2021)	-
Airbus D&S	Netasq (2012), Arkoon (2013)	-
BAE Systems	Detica (2008), Stratesc (2010), ETI A/S (2010), Intelligence BU of L-1 Identity, Norkom (2011), Silversky (2014)	-
Leonardo	Vitrociset (2019)	-
Rohde & Schwarz	GateProtect (2014), Adyton Systems (2014), Sirrix (2015), R&S Cybersecurity HSM (2016), DenyAll (2017), Camero-Tech Ltd (2019)	-

They enjoy a better competitive environment on their domestic market (where digital SMEs and key players are essentially foreign). In France for example, according to the French ACN Digital Trust observatory, Thales and Airbus Defence and Space are the two main players in the sector, generating €1.66 billion and €520 million in revenue in this field respectively[31]. They are ahead of specialised companies such as Atos, Idemia and IBM France.

They have mainly gained this position through company buyouts completed over the last ten years. Thales, BAE Systems and Rohde & Schwarz stand out for their dynamic activity in this area. The British group BAE Systems invested almost £1 billion between 2008 and 2014 in the acquisition of six firms which allowed it to create its “Cyber & Intelligence” division (8% of 2020 revenue). The German group Rohde & Schwarz, which posted total revenue of €2.34 billion in 2020, conducted its acquisition policy between 2014 and 2019, targeting six firms.

[29] “General Dynamics completes CSRA acquisition”, *Defense News,* 3 April 2018.

[30] Kévin Martin, “Europe et cybersécurité : quelle(s) base(s) industrielle(s) ?”, *Revue Défense Nationale*, 2019/4, no. 819, pp. 107-113.

[31] ACN, Observatoire pour la confiance numérique, 2021, p. 3.

Over this period, the group's revenue grew by more than 20%, its workforce by more than 30% and it reorganised its operations in four business units (Aerospace and Defence Security, Cyber Security, Test & Measuring, Broadcasting and Media).

In 2016, Thales initiated a digital transformation policy. Cyber security, AI, Big Data and IoT/connectivity are explicitly identified as the four technology pillars underpinning this transformation[32]. The group is asserting its ambitions via a security approach. In addition to internal reorganisations[33], this policy has led to a wave of strategic buyouts in France and the US. Thales particularly took over the cyber business of Alcatel Lucent in 2014 and then made two successive acquisitions in the US targeting Vormetric (2015) and Guavus (2017). The buyout of Gemalto for €4.8 billion initiated in 2017 and finalised in 2019 marks the culmination of this policy with the creation of a new dual-use business division "Digital Identity and Security". It accounted for 18% of revenue in 2020.

Airbus Defence & Space (two acquisitions consolidated within the subsidiary Stormshield) and Leonardo (buyout of the avionics specialist Vitrociset) have tended to merge their traditional cyber security businesses within dedicated divisions, reflecting their firmly rooted positioning in defence. For Airbus Defence & Space, they are concentrated in the Connected Intelligence entity[34] and for Leonardo, in the Cyber Security division which is part of the Defence, Electronics & Security Business Unit.

[32] "Thales présente ses grandes priorités stratégiques 2018-2021 lors de sa journée investisseurs", *Thales Press Release,* 6 June 2018.

[33] In 2011, the group began an internal reorganisation of its digital businesses (cyber security, identity, etc.) and created Thales Communications & Security after merging Thales Communication (specialising in secure information and communication systems and products) and Thales Security Solutions and Services (security of citizen systems, critical infrastructure and passengers). In 2013, it reorganised the group's businesses around a new model based on six Global Business Units (GBU), themselves grouped together in three operational sectors (Defence & Security, Aviation and Transport). In this context, the Secure Information and Communications Systems division is part of the Defence & Security sector. In 2014, Thales integrated its expertise in information systems security and critical information systems to form a new segment called "Critical Information Systems and Cyber Security".

[34] Note that Airbus D&S has retained its subsidiary Stormshield, thereby keeping its specific sales channel.

Figure no. 8: CYBER SECURITY BUSINESSES WITHIN AIRBUS D&S AND LEONARDO[35]

IN € MILLION	FY 2020
Order Intake (net)	11,862
Order Book	33,505
Revenues	10,446
R&D Expenses	225

Military Aircraft 56%
Space Systems 24%
Connected Intelligence & Others 20%

Connected Intelligence includes five main business clusters: Secure Communications, Intelligence, Cyber Security, Security Solutions and Secure Land Communications. These clusters develop specific solutions for defence, governmental, civil and commercial customers;

Airbus D&S

Leonardo

3.3. Privileged partnership strategy for Artificial Intelligence and Big Data technologies

This external growth strategy was apparently favoured by defence companies in the cyber security sector during the 2010-2017 period and brought new business opportunities (both retained and otherwise). With the wave of AI-related technologies that are vital to optimise the performances of existing solutions, defence companies sought more to reinforce their internal capacities. In the US, the main historical defence players strengthened their R&D activities in autonomy and robotisation, and took advantage of the launch of several DoD programmes in this field.

The emphasis is also on partnerships. In recent years, defence companies have changed their innovation systems and organisations to create an appropriate framework for cooperating in digital technology, such as AI, with specialised firms from the industrial and research ecosystem. Following the philosophy of open innovation, this strategy aims to attract digital start-ups and keep abreast of technological developments (creation of accelerators, incubators and technology challenges). However, the relationships developed upstream do not necessarily lead to a lasting industrial and business partnership.

These initiatives rely on corporate venturing. While the practice is not new[36], it seems to be very popular with defence companies, especially with the explosion of digital technologies[37]. Chris Moran, head of Lockheed Martin Ventures sums up the role of corporate venturing for a defence company as a means of detecting emerging, mainly dual-use technologies and

[35] Taken from Airbus SE and Leonardo Company 2020 presentations and registration documents

[36] "Why defense giants tie in with start-ups. `Partnering' gives high-tech access or paths apart from Pentagon", *The Christian Science Monitor*, 16 April 1986.

[37] "Defense Industry Adds Venture Capital to Its Arsenal", *Wall Street Journal*, 5 July 2018.

acquiring interests in innovating start-ups. The investment, which is exclusively as a minority shareholder, aims to guide the start-up towards solutions that meet defence needs while retaining the firm's business model and potential business opportunities[38]. In the United States, Lockheed Martin Ventures was set up in 2007 (but the fund has only been really active since 2016[39]) whereas Horizon X (Boeing) and Honeywell Venture Capital were launched in 2017. The movement is similar in Europe. Although corporate venturing has existed for several years within the main defence companies[40], Safran and Airbus Group Ventures launched their entities in 2015. MBDA made a similar move in 2017[41].

A note by the Center for Security and Emerging Technology (CSET) confirms that defence companies with a corporate venture fund tend to take minority interests in AI technologies, rather than opting for buyouts[42]. Through this partnership approach, their corporate venture entities find a position alongside specialised funds, even though their financial capacities and investment objectives differ[43]. But alliances are a possibility, as seen with Boeing's decision in August 2021 to join forces with AE Industrial Partners. Its corporate venture fund thus became a spin-off, through an agreement signed with the specialised investment fund[44]. The decision gives Horizon X more capital – and therefore greater capacity to invest – while Boeing retains a majority stake in the entity. Defence companies may also acquire an interest in specialised seed funds, like Naval Group for example (PSL Innovation Funds)[45].

[38] Chris Moran: "*At Lockheed Martin Ventures, the first thing we do is screen the emerging technology we're looking at against the business interests of the corporation. We are looking for what we call 'dual use' technologies. However, we're not a huge fund. We're a $200 million fund, and we aim to be a minority shareholder in technology startups. Lockheed Martin Ventures wants to tap into these startups, and ultimately serve as a [market/ bridge] for the emerging technology being created outside the walls of the defense industry. Being a minority shareholder means companies will have the space to sell to the entirety of the aerospace and defense sector. That's a scenario where everyone wins*". Cf. "Lockheed Martin seeks investments not acquisitions in dual-use technology startups", Lockheed Martin, July 2020.

[39] As a result of a new organisation with the appointment of Chris Moran to head up the entity. Cf. "With new hire at helm, Lockheed Martin Ventures readies to make first investment", *Inside Defense*, 9 September 2016.

[40] For instance, Saab Coporate Venture was launched in 2001.

[41] Cf. MBDA, *Corporate & Social Responsibility Report 2017,* May 2018, p. 18. "*In 2017, we increased our engagement in Open Innovation. We set up a corporate-venture capital activity and started to invest in new promising technologies developed by start-ups and small and medium-sized enterprises (SMEs*)".

[42] Ngor Luong, Rebecca Gelles, Melissa Flagg, "Mapping the AI Investment Activities of Top Global Defense Companies", *CSET Issue Brief,* Center for Security and Emerging technology, October 2021.

[43] "How corporate defense venture funds fit into the VC ecosystem", *Defense News,* 30 January 2020.

[44] "Boeing to spin off venture capital arm HorizonX", Reuters, 5 August 2021.

[45] "Naval Group soutient le lancement d'un fonds d'amorçage dédié aux startups", *Mer et Marine*, 29 June 2018.

Figure no. 9: INVESTMENTS AND ACQUISITIONS IN AI BY DEFENCE COMPANIES: A FEW EXAMPLES (2013-2020)

Companies are ranked by the number of AI investment transactions.

COUNTRY	DEFENSE COMPANY	INVESTMENTS AI	INVESTMENTS Non-AI	M&A AI	M&A Non-AI
Netherlands/France	Airbus	19	38		
United States	Honeywell	7	14		
United States	Lockheed Martin	7	31		
United States	Science Applications International Corp.	6	13		
United States	Boeing	5	30	1	10
South Korea	Hanwha	2	14		
Israel	Rafael Advanced Defense Systems	2	12		
United States	Huntington Ingalls Industries	1		1	1
United States	Jacobs	1			
United States	Northrop Grumman	1			
France	Safran Corporate	1	9		
United Kingdom	BAE Systems		2	2	6
United States	United Technologies Corp.		2	1	1
United States	General Dynamics Corp.			1	3
	Total	52	165	6	21

Source: Center for Security and Emerging technology (CSET)

More conventionally, defence companies have pursued a policy of initiating partnerships with specialised players, the aim being to jointly develop an offering integrating AI or big data capacities that the company will market. The partnership, which is part of a defined industrial and commercial project, can be carried out in two complementary ways:

- with leading digital technology players taking part in the digital transformation of the company and its business;
- with players of all sizes (major firms, mid-caps, SMEs and start-ups), mainly specialising in applications.

This is the case of Airbus Group which has engaged in data collection in order to develop new fleet management and predictive maintenance services. This has led to the new offerings called “Skywise” (for civil aviation platforms) and “Smartforce”[46] (military aviation platforms), both developed in partnership with specialised players like Palantir and Alten. In

[46] “Airbus launches SmartForce – services bringing the power of data to military operations”, Airbus Defence and Space, 16 July 2018.

2018, Lockheed Martin and Amazon Web Services signed a strategic partnership in ground station service activities after founding AWS Ground Station[47].

In addition, as part of the development of a secure cloud computing offer for armed forces and public institutions, European defence companies have teamed up with leading players in the field. Thales[48], Leonardo[49] and Fincantieri[50] have respectively joined forces with Google Cloud, Microsoft and Amazon Web Services to secure a position in their national public cloud market. Thales and Microsoft are also partnering to develop a defence cloud solution called Nexium Defence Cloud[51].

Conclusion

The actions taken by defence companies in digital technology not only meet the needs of their internal digital transformation, but also respond to a change in their business, be it their core business or as part of a diversification strategy. With this adaptation, several issues arise, primarily the particularly intense competition from predominantly commercial companies, which may be key digital players or new entrants. This is a new state of play brought about by the place that digital innovations have taken in the definition of new defence needs and in optimising the performance of existing defence systems and equipment.

In some mature fields of technology, such as cloud infrastructures and related services, the lead gained by key digital players and the size of the necessary investments mean that defence companies must at least pursue a partnership strategy in order to develop joint offerings for their traditional customers (armed forces and public institutions). But they now face the very real risk of being ousted from new, large-scale markets.

In areas in which technology is less mature, such as non-machine learning AI ("explainable" AI, etc.) or quantum computing, defence companies are focusing on R&D while developing their interaction with the most innovative civil ecosystems. They aim to benefit from progress in civil technology as soon as possible, without being dependent on key digital players. However, this requires them to redefine the traditional prime contractor – subcontractor relationship, with companies that do not always come from traditional defence industrial or technological bases. This is also a major issue for Armed Forces and national Defence Ministries, which are seeking to capture innovations from these new players for the benefit of arms programmes via an incremental approach.

---

[47] "Amazon-Lockheed venture casts shadow on ground station startups", *Space News,* 29 November 2018.

[48] "Thales et Google Cloud annoncent un partenariat stratégique pour développer conjointement un 'Cloud de Confiance' en France", Press release, Thales Group, 6 October 2021.

[49] "Leonardo and Microsoft: a new partnership for a secure digitization of public administration and national infrastructures", Press release, Leonardo company, 26 May 2021.

[50] "Fincantieri and Amazon Web Services team up to power the digitization and competitiveness of Italy with cloud computing", Press release, Fincantieri, 13 May 2021.

[51] "Thales and Microsoft partner to develop a unique Defence Cloud solution", Press release, Microsoft, 12 June 2018.