MAY 2022

CIO letter

Thomas FRIEDBERGER
Deputy CEO
Tikehau Capital and Co-CIO

Gilles DAGUET
Managing Director
Private Equity - Tikehau Capital

François LAVASTE
Executive Director
Private Equity - Tikehau Capital

CYBER, FROM SECURITY TO RESILIENCE

In 2021[1], two thirds of the world population owned a mobile phone (5.2 billion people out of a total of 7.8 billion), 60% of humanity (4.7 billion people) had access to the internet and more than half were active on social media (4.2 billion people). It is not too bold a claim to assume that, in 2022, almost 100% of businesses around the world will be working with computer systems. For these businesses, "digitalisation of processes" for producing goods and services, for distribution, and necessary processes for relationships with customers and suppliers or supply chains is an essential requirement and a key factor of competitiveness. In two years' time, e-commerce is expected to account for a market worth more than $800 billion, propelled by the arrival of the "Metaverse" and non-fungible tokens (NFTs)[2]. For governments, the challenges of "digitalisation" also include the need to modernise how public services operate and to improve their efficiency, from job-seeking services to healthcare, education and tax payments.

In this regard, the challenges of cybersecurity are monumental. For something that, on the one hand, is necessary for modernisation and represents a competitive advantage or a feature of economic development, it also appears to be an extraordinary source of vulnerability if systems and data are not well protected. We can therefore conclude that cybersecurity risks, alongside issues of public health and climate change, likely feature amongst those that affect the highest number of human beings on the planet. This is probably why in April 2021, the Chair of the US Federal Reserve cited cyber attacks as the greatest risk to the stability of the global economic system. According to a report by the World Economic Forum, cyber risk was the threat that increased more than any other during the COVID-19 crisis[2]. From a European perspective, the expected inclusion of cybersecurity in the European social taxonomy is proof that this sector is central to building more resilient ecosystems[3].

We are therefore focussing on this topic in our letter. Not only because this subject is of paramount importance for the companies we invest in, as well as for our partners, suppliers, investors and shareholders, but also because, since **we have identified this trend as one of the most significant investment opportunities for the next few decades**, we have unparalleled expertise in Europe. We provide this unique knowledge through an experienced investment team managing the largest private equity fund dedicated to cybersecurity in Europe. It is together with said team that we are writing this letter, to share our approach to such a key topic with our readers.

1. wearesocial.com
2. The Global Risk Report World Economic Forum 2022
3. ec.europa.eu

TIKEHAU CAPITAL

Cyber risk

Cyber attacks are attempts to damage a computer system which are carried out with malicious intent. They target various computing devices: computers and servers, both remote and networked ones, either connected to the internet or not, peripheral equipment such as printers, or even communication devices such as mobile phones, smartphones and tablets. More recently, as industry becomes more digital and with the introduction of connected vehicles, these attacks may also compromise the integrity of machine tools, factories and our cars. There are four types of cyber risks, each with different consequences, which affect individuals, authorities and companies both directly and indirectly. Cybercrime refers to obtaining personal data in order to exploit or resell it. Image infringement refers to editing the appearance or content of a site, thereby altering the integrity of its web pages. Espionage relates to the targeted acquisition of economic, political, military or scientific data. Finally, sabotage is the act of rendering all or part of an organisation's information system inoperative via a cyber attack. Cybersecurity encompasses all the measures put in place to protect against these risks. In particular, it combines the following: security of networks, the cloud, workstations, mobile phones, infrastructures and connected objects; detection of threats, intrusions and fraud; access and identity management; intrusion tests; and email and web filtering.

> **IF CYBER RISK WERE AN ECONOMY, IT WOULD BE THE THIRD LARGEST IN THE WORLD.**

The *Club des Juristes* think tank[4] estimates that global cyber risk accounted for $6 trillion in 2021. If cyber risk were an economy, it would be the third largest in the world, behind the United States and China. This figure is expected to rise to $10.5 trillion by 2025, a growth rate of almost 15% per year[5].

The COVID-19 crisis, which saw a fast increase in an enormous number of people working from home and shopping online, has only amplified cyber risk. It also demonstrated how vulnerable our healthcare systems are to cyber attacks, which are not only capable of stealing or

4. leclubdesjuristes.com
5. Cyberwarfare in the C-suite, Cybersecurity ventures, January 2021 and Report from the French Ministry of the Interior, the State of the Digital Threat *(État de la menace numérique)*

falsifying massive amounts of data, but also incapacitating a hospital system under extreme strain. The Russia-Ukraine crisis is further exacerbating the risk. In a press release from 21 March 2022[6], the White House reiterated their warnings about the incredibly high likelihood of cyber attacks. They stated that the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) is actively working alongside critical infrastructure organisations to quickly share information and advice on threat mitigation measures to help them safeguard their systems and networks.

According to the United Nations, the number of malicious emails circulating worldwide increased by more than 600% at the start of the COVID-19 pandemic[7]. The US Federal Bureau of Investigation (FBI) has warned that there are now 100 different strains of ransomware in circulation around the world. There were on average 270 attacks per organisation in 2021, an increase of 31% from 2020[8]. The amount of money stolen by hackers increased fourfold between 2019 and 2020. In the US, the FBI received almost 800,000 reports of cyber incidents in 2020[9] and surveys suggest that more than half of all businesses have been the victim of a cyber attack[10]. On average, it takes a company 280 days to resolve a cyber attack[11].

To date, the single most destructive cyber attack was the NotPetya attack in 2017. It was originally directed at Ukrainian organisations, but the collateral damage

> **THE AMOUNT OF MONEY STOLEN BY HACKERS INCREASED FOURFOLD BETWEEN 2019 AND 2020.**

associated with this computer worm's ability to automatically replicate itself in computer networks was felt around the globe. This attack is estimated to have inflicted over $10 billion in damage, just over 10% of Ukraine's GDP at the time. In November 2021, the cloud cybersecurity team at Chinese company Alibaba disclosed a vulnerability in the Java-based logging utility Log4j, an open-source framework that allows software developers to log a variety of data within their application. In the week following the Log4Shell vulnerability announcement, more than 100 exploit attempts per minute were reported.

Cyber criminals take every opportunity to exploit vulnerabilities in people and organisations through the use of technology. They are quick to adopt new technologies, they adapt their attack strategies using new approaches and they cooperate with each other. Organised

6. whitehouse.gov
7. abcnews.go.com
8. Global Cybersecurity Outlook 2022 – World Economic Forum
9. IC3, "Internet Crime Report 2020", 2021
10. The economic impact of cyberattacks – Goldman Sachs US economics analyst, 7 March 2022
11. IBM Security. 2020. Cost of a Data Breach Report 2020 – ibm.com

IN THE US, THE PRICE OF CYBER INSURANCE ROSE BY ANNUAL RATE OF

204%

IN 2021

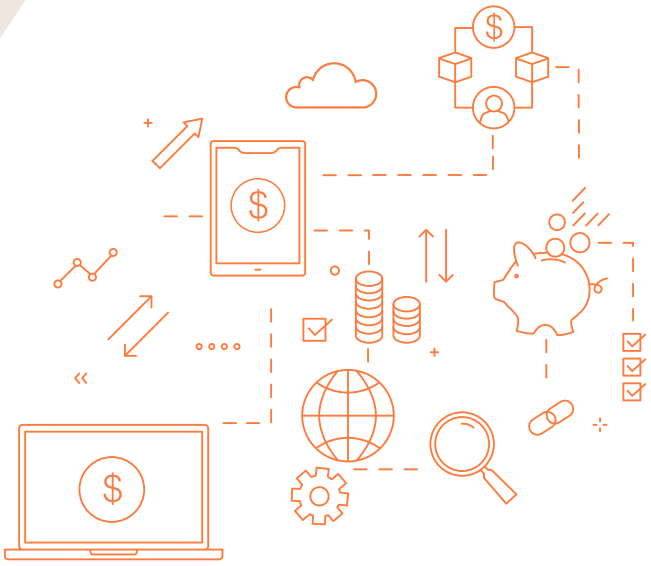
crime has quickly added a digital angle to its arsenal. Europol recently reported that organised crime groups are recruiting hackers for phishing or to send malware in order to gain control over victims' bank accounts. In addition, organised crime groups often involve cyber criminals in legal business operations, blurring the lines between legal and criminal business. These individuals can be based anywhere in the world, which prevents law enforcement authorities from intervening in these groups' activities.

Insurance is one of the preferred solutions for companies to minimise the impact of cyber incidents[12]. The majority of companies have cyber insurance, either to limit financial liability for specific cyber incidents or to benefit from incident response services and professionals provided by the insurance company. However, the maturity stage of cyber insurance markets varies considerably from country to country. In some regions, it is common practice. In others, it is a solution that has only just begun to appear. Moreover, the cyber insurance industry is undergoing a major change. Due to emerging ransomware attacks and the sheer number of them, premiums increased by 180% on average in 2021. In the US, the price of cyber insurance rose by an annual rate of 204% in 2021[13]. In an article published in the French financial newspaper "Les Echos"[14], the head of insurance risk management at Airbus Defence and Space pointed out that, between 2019 and 2020, cyber attacks cost insurers three times as much money in one year. These attacks caused insurers to spend significantly more on compensating their policyholders than they received in premiums, despite the increase in these premiums. He warned: "We are very close to a vicious circle being triggered in the market of cyber insurance for businesses. It could lead to insurers having less and less capacity when companies need them more and more". The loss ratio, a profitability indicator for insurers, did indeed rise from 84% in 2019 to 167% in 2020, according to the French risk management association AMRAE[15]. In addition, when insurers make ransom payments, this bolsters the resources available to cyber criminals, creating a vicious circle that highlights the limitations of insurance contracts in this field.

12. Global Cybersecurity Outlook 2022 – World Economic Forum
13. Invest Quarterly Sector Outlook: Information Security, 4Q21, Frank Marsala, Gartner- The Global Risk Report World Economic Forum 2022
14. Les Echos – les cyberattaques coûtent trois fois plus aux assureurs en un an, 26 May 2021
15. Association pour le Management des Risques et des Assurances de l'Entreprise – amrae.fr

A unique investment opportunity

The COVID-19 crisis and the subsequent Russia-Ukraine war have underlined the incredible vulnerability of an economic model that is aimed at achieving growth in the short term. Low interest rates have allowed governments to give massive support to the global economy through aggressive fiscal policies financed by a significant increase in debt stocks. In other words, relying heavily on debt has made it possible to extend the economic cycle but has, in return, made generating short-term growth necessary in order to justify these levels of leverage. However, reversing three long-term trends at the same time, which have served as a tailwind for the growth of corporate earnings over the last thirty years, now threatens this delicate balance: interest rates have likely reached a low point, as have corporate tax rates. Globalisation on the other hand has marked a turning point which no longer allows companies to take an overly optimistic view of their production costs, taxation or the levels of capital they operate with. East-West rivalry weakens the globalised business model, which benefits from making an overly effective use of its supply chain and industrial process by carrying out production where costs are lowest. Moreover, the rise in two types of standards and norms, two different monetary systems and the closure of potential markets due to choosing either one side or the other will force companies to invest heavily in system security. To remain competitive and build resilience in response to these disincentives to generate financial returns, companies will need to make significant investments, beginning a new cycle of capital expenditure. This cycle has already begun in some areas, such as the United States, where the government has chosen to help companies relocate their production and safeguard their supplies and information systems. In this respect, cybersecurity appears to be one of the three areas, together with



energy efficiency and the "digitalisation" of production processes, that companies around the world need to invest in heavily to minimise their vulnerability and increase their resilience. Governments and public services will follow this trend. The crisis in Ukraine is expected to trigger an enormous increase in cybersecurity budgets for all organisations. Opening the use of data up to the masses, decentralisation of payments and "digitalisation" of processes make cyber investments essential. These are not tactical investments, but strategic choices made at the general management level of companies, and they concern every department in the organisation across all areas of activity.

The capitalist economic model, based on the expectation that profit will be generated by the private sector, constantly seeks to achieve the scale effect, which allows the profit-making capacity of a process to be multiplied. In the 20th century, this scale effect was made possible by using oil as the main source of energy, as well as by deregulating and globalising the economy after the collapse of the communist model in the late 1980s. **In the 21st century, this scale effect is made possible thanks to digital technologies and the ability of products, services and brands to reach the entire global population through communication devices. Cyber risk threatens this entire economic model.**

The alarming outburst in the number of ransomware attacks and their increasing degree of sophistication around the world illustrates the urgent need for economic agents to establish ambitious investment plans in order to defend themselves and ensure their resilience and durability. This is not only to protect intellectual property and data, but also to safeguard jobs that would be at risk if the organisation were to find itself unable to operate or suffer financial loss. In a study published by PricewaterhouseCoopers[16], the majority of business owners surveyed expected a significant increase in cyber risk in areas as diverse as attempted virus intrusions (malware), ransom demands (ransomware), supply chain disruptions, disinformation, state-sponsored attacks on critical infrastructure and exercising influence on corporate research and development. More than 25% of business owners expect double-digit growth in cyber budgets in 2022. This is even more significant as companies with the best organisations in this field, i.e., managers with commitment to cybersecurity, a good level of data reliability and a well performing organisation, have much more room for growth in the cyber domain than others.

16. 2022 Global Digital Trust Insight, PwC

THE GLOBAL CYBER ECOSYSTEM EMPLOYS

3.5 M

PEOPLE BUT LACKS ABOUT 3 MILLION ADDITIONAL EMPLOYEES

However, the cybersecurity sector is made up of a large number of start-ups and medium-sized non-listed companies financed by private equity funds. These are mainly American, although Europe and France in particular feature amongst the leaders in unlisted investment in the sector. As well as these small companies, a limited number of large listed groups complete the cybersecurity ecosystem. This rapidly growing ecosystem is therefore not mature. Just like the transition to renewable energy, the sector represents a megatrend that makes it a unique investment opportunity. The global cyber ecosystem employs 3.5 million people but lacks about 3 million additional employees[17]. Universities will struggle to train such a large number of specialists in a short space of time. This is something that will exacerbate the critical need to automate cyber processes and focus on artificial intelligence to make up for the lack of human specialists. The need for investment in this area is therefore enormous.

The industry needs the contribution of technology in order to improve its production processes. Not only to make them more efficient, but also more in line with the pursuit of sustainable growth. The opposite is also true. Technology needs the industry in order to be relevant and connect with people. In a previous letter[18], we mentioned the risks of rising inequalities as a result of technological progress. We also mentioned the risk of society becoming compartmentalised as a consequence of the filter bubbles that tech enables: internet users are recommended content in keeping with their views and beliefs, which leads to withdrawal into distinct communities and makes it harder to prevent debates and dialogue from breaking down. **Tech therefore needs to find a way to reintroduce humanity into all its forms. Its contribution to making the industry more durable and more of a community, and to giving it a genuine competitive edge for regional ecosystems, is one of its redeeming qualities and likely forms part of the idea behind the "Tech for Good" movement. This cannot be achieved without involving cybersecurity.**

17. weforum.org
18. Tikehau CIO letter – Robot Rock, March 2021

What this means for businesses

The problem for business leaders is that cyber threat changes and adapts all the time, which means you can never assume that protection measures put in place at any one point in time will guarantee future security. 95% of cybersecurity issues are linked to human error[19]. The question that arises is really "when" and "how much" a company will be affected, rather than "if" it will be. Furthermore, cybersecurity is not just a concern for an organisation's IT department, as an attack can seriously affect the continuity of the entire company. It is therefore a key issue which must be dealt with at the level of the Executive Committee and the Board of Directors, and which all employees must be made aware of and trained for. Consequently, in order to establish best practices, companies need to map cybersecurity risks, the potential impact of attacks, structural damage and to prioritise where to direct their efforts accordingly. A business continuity and disaster recovery plan should also be put in place and a cybersecurity drill should be organised at least once a year, just like fire drills.

A company is only as secure as the weakest link in its ecosystem. Cyber attacks against other organisations in the digital supply chain can negatively impact downstream businesses and their operations. In 2021, ransomware group REvil exploited a vulnerability in a remote monitoring and management software platform and launched one of the largest ransomware attacks

19. Invest Quarterly Sector Outlook: Information Security, 4Q21, Frank Marsala, Gartner. The Global Risk Report World Economic Forum 2022: CHAPTER 3 Digital Dependencies and Cyber Vulnerabilities

in history, affecting the platform's entire supply chain[20]. The attack disrupted nearly 1,500 businesses worldwide, including a Swedish grocery chain, which forced more than 800 stores to temporarily close[21]. Over the past few years, successful indirect attacks have risen from 44% to 61%[22]. In addition to focusing on their own information systems, companies must therefore also think about the resilience of their entire chain of partners, customers and suppliers.

In terms of the cost to businesses, a study by the Council of Economic Advisers (CEA) estimated that large, listed companies lost an average of almost $500 million in value per adverse cyber event[23]. During the health crisis, attackers focused on low-risk, high-reward opportunities, forcing companies' cybersecurity teams to work tirelessly to protect their organisations from persistent threats. Cybersecurity teams need to equip themselves to keep up with evolving threats, have visibility in both their own networks and the extended networks of their supply chains and third-party ecosystems, and above all retain talent. However, not only is there a global shortage of cybersecurity talent, but it is also not clear whether talented professionals in this area can adapt to a business environment. In an interview on the YouTube channel Thinkerview[24], two French "ethical hackers" describe, not without some humour, the difficulties that companies encounter in recruiting talented professionals with their profile: they're not willing to write CVs, there has to be a nap room at the workplace to make night shifts easier, no fixed hours, etc.

OVER THE PAST FEW YEARS, SUCCESSFUL INDIRECT ATTACKS HAVE RISEN FROM 44% TO

61%

20. Global Cybersecurity Outlook 2022 – World Economic Forum
21. Klugerman, Yaffa. 2021. The 5 Most Notable Third-Party Data Breaches of 2021 (So Far). Panorays
22. Bissell, Kelly, et al. 2021. State of Cybersecurity Resilience 2021. Accenture
23. Economic report of the president – White house – 2018
24. Hacking in the 21st Century – Thinkerview, September 2021

Cybersecurity is a concern for all companies, large or small, and for all players in the global economy in general, including governments. Funding channels for the sector are therefore of key importance. It is absolutely vital for Europe to enable cybersecurity companies to stay in the region by providing effective financial support to allow them to thrive, in order to avoid an exodus to the deep American capital markets. Cybersecurity highlights the dire need for an effective industrial policy based on partnerships between states and their industrial ecosystems, and illustrates the key issues surrounding the technological revolution we are currently experiencing.

In this respect, it is unsurprising that investors in private equity funds in cybersecurity are also the companies themselves, for the same strategic reasons. These investments allow them to understand and access the expertise of companies raising capital through these funds.

THE UNITED STATES ACCOUNTS FOR MORE THAN

80%

OF THE FUNDS RAISED.

> **“**
>
> **CYBERSECURITY HIGHLIGHTS THE DIRE NEED FOR AN EFFECTIVE INDUSTRIAL POLICY BASED ON PARTNERSHIPS BETWEEN STATES AND THEIR INDUSTRIAL ECOSYSTEMS, AND ILLUSTRATES THE KEY ISSUES SURROUNDING THE TECHNOLOGICAL REVOLUTION WE ARE CURRENTLY EXPERIENCING.**

2021 was a record year for capital raising in private equity dedicated to cybersecurity. In total, more than $21 billion was raised by 727 companies, more than three times the amount raised over the previous three years combined. The United States accounts for more than 80% of the funds raised, with Israel and Europe jointly accounting for about 15%. In Europe, the United Kingdom remains in the leading position by a large margin, ahead of France, Germany, Spain and Switzerland.

Joep GOMMERS
CEO and founder of EclecticIQ, a Tikehau Capital portfolio company

Prior to launching EclecticIQ in 2014, he worked in the cyber threat intelligence field for iSIGHT Partners.

At EclecticIQ, we are privileged to support the most targeted organisations in the world by managing, sharing and acting on information in the field of cyber threats. This enables national security organisations and enterprises to prevent, deter and defeat cyber threats. This article aims to provide executives with guidance as they work alongside their cybersecurity teams to shape high ROI cybersecurity programs that are in line with the reality these threats pose.

UNDERSTANDING YOUR ENVIRONMENT TO UNDERSTAND THE RISKS

Managing risk means managing uncertainty around your business objectives which, by definition, makes managing cybersecurity risks a board concern. This uncertainty is influenced in large part by the environment you operate in. Without a clear understanding of the environment, the cyber threat actors operating within it and their (malicious) intent and capabilities, it is almost impossible to comprehend the level of risk you face, let alone take the appropriate action and remain in control.

THE THREAT LANDSCAPE HAS EVOLVED AND SO SHOULD YOUR APPROACH

Many years ago, a deep understanding of your business, its processes, IT systems and weaknesses was all that was needed to shape security controls in order to manage risk. With a known and manageable quantity of potential cyber threats, simply being aware of how they could affect your organisation was enough. In today's world, where cyber threats are constant, prevalent and rapidly evolving, it is impossible to protect yourself against all possible permutations of cyber threats and threat vectors. For a high return on investment in managing cyber risk, it is imperative you ensure your investment reduces the uncertainty on your business objectives as much as possible. This means that your efforts and investments in cybersecurity should not rely solely on insights into your own organisation, but decisions should also be informed by the existing, wider threat landscape you are facing. Aligning cybersecurity efforts and investment with your threat reality drives return on investment which, ultimately, reduces the uncertainty around your business objectives and lowers risk accordingly.

Understanding the threat landscape you are facing is not as straightforward as it sounds. Nor is translating this understanding into operational activities and, ultimately, business value. Cyber threat intelligence comes in many different shapes and sizes; making the right choices and ensuring it is appropriately implemented makes a great difference between wasteful investment and return on investment in cybersecurity.

A 4-STEP APPROACH TO SHAPE RISK MANAGEMENT AND REDUCE THREATS

As an executive decision maker, you will be working with your cybersecurity teams to shape risk management and reduce threats with Cyber Threat Intelligence. The 4 topics below should be part of the agenda for discussion with your teams. Think holistically. Connect with your community. Obtain the right intelligence. Take action.

Think holistically. We often default to working exclusively with operational cybersecurity teams who have an immediate need to detect or respond to malicious activity. However, trying to reduce the risk from cyber threats requires a more holistic approach. Preventing a disadvantageous situation from developing may require action within the business itself. Prevention is often strategic, so you should ensure that risks, compliance, and legal and business stakeholders are well represented in any efforts to implement threat intelligence into your business. When it is too late for prevention, we must stop malicious threats in their tracks and "deter". This means relying on the involvement of IT and Security Architects and your operational security teams, such as security operations and incident response specialists. Because, when all else fails and you face an incident, which WILL happen, you must make sure you guarantee a successful outcome and end this "conflict" on favourable terms. Ensure your program addresses the needs of your stakeholders across the spectrum of "prevention, deterrence and defeat" – strategically, tactically and operationally – and have an understanding of how they want and can use threat intelligence.

Connect with your community. Most organisations face the same threats in isolation, wasting time and resources on threats and responding to incidents that are commonplace or prevalent in their sector. Close cooperation with local National Cyber Security Centres and/or Sector Computer Emergency Response Teams and other community initiatives is great for bootstrapping your information position. Ensure cooperation through knowledge sharing, operational consumption and by exchanging information on threats and incidents.

Obtain the right intelligence. Contrary to intuition, proactivity is a more worthwhile pursuit than intelligence about an immediate threat. Immediate relevancy usually means you are already exposed; preventing that exposure to begin with should be your top priority. This does not mean you should avoid pursuing intelligence on threats that affect you immediately and directly. External footprint monitoring, discovering rogue and exposed assets, monitoring for credential and intellectual property leakage and brand abuse should be a part of your program.

Your focus should nevertheless be on obtaining intelligence that informs you about the capabilities and modus operandi of threat actors who, at first sight, are in opposition to your objectives and who target organisations like your own; targeting the technologies you possess,

your sector or the (geographical) communities you are part of. You want to obtain information about threats that have already materialised elsewhere, where reactive efforts from others enable your abilities to be proactive, or obtain information about the underlying capabilities of these actors so you can detect threats that have so far not materialised elsewhere. Specifically, you want access to Indicators of Compromise (IOCs) and detection rules that allow you to detect known infrastructure and cyber threat tools. However, with rapidly changing threats, the relevance of IOCs is quickly diminishing and they need to be reinforced with more robust insights that remain relevant as threat actors rotate the tools and infrastructure they use. You should ensure intelligence about the underlying capabilities and the Tactics, Techniques and Procedures (TTPs) that threat actors use is available. These capabilities and their modus operandi – just like the workings of a business – are often harder to change for cyber threat actors. Business, IT and Security Architects can use this understanding to put controls against these capabilities in place or to tweak processes and systems to minimise the potential impact of the attack chains – that combine multiple capabilities – used by threat actors.

Take action. Availability of intelligence does not mean that is it used and leveraged by the correct parties. Leveraged does not mean understood. Understood does not mean actioned, just as actioned does not mean effective. Acting on intelligence, like acting on a customer issue, means making sure the ball is not dropped, ensuring it makes it to the right place in the organisation and that action is taken. For different parts of the organisation, taking action will mean different things and will require different steps to be taken. Some forms of risk, management and areas of the business will require briefings or written versions of intelligence to be distributed, and operational teams will require aggregation, analysis and automation tooling. Understand the structure of people, processes and technology that is required in order for the relevant parts of the organisation to act accordingly. Be realistic when implementing steps towards your end goal.

The cyber ecosystem

The partnership between governments and companies is key to fostering an ecosystem that promotes cybersecurity. In some leading countries, the partnership between the army and private companies even represents a significant competitive advantage. It is therefore unsurprising that the leading countries in cybersecurity are all significant military powers: United States, China, Russia, Israel, United Kingdom and France. **On the one hand, capitalist economies benefit from liquid and deep capital markets which make it possible to raise significant amounts of money. On the other hand, economies characterised by greater state ownership, such as Russia or China, can benefit from the effects of long-term planning to develop their cyber ecosystem.**

In Israel, the general director of the venture capital firm Team8[25] talks about an "unfair advantage", because of how important a role the army plays in supporting the development of private companies in the sector. In the Israeli army, Unit 8200 recruits the best students to perform their military service through working in cybersecurity. Unit 8200 is an intelligence unit of the Israel Defense Forces, which is responsible for signals intelligence and code breaking. According to the Director of Military Science at the Royal United Services Institute, a British defence and security think tank, "Unit 8200 is probably the best technical intelligence agency in the world and is on par with the NSA in all respects, except for its scale."[26] After their military service, the young entrepreneurs are welcomed by the Team 8200 unit's equivalent in business, Team8, to help them found and develop their own companies. Cybersecurity was declared a national priority in 2010. In the decade since, Israel has become one of the world leaders in the field. There are now more than 300 active start-ups in the country, along with two of the ten most important companies in the sector worldwide. 20% of global private investment in cybersecurity goes to Israeli companies and more than 30 multinational companies have already set up their cyber research and development centres in Israel[27]. The city of Beersheba, located in the middle of a semi-desert area of the country, is now the country's

20%

OF GLOBAL PRIVATE INVESTMENT IN CYBERSECURITY GOES TO ISRAELI COMPANIES.

25. team8.vc
26. fr.wikipedia.org
27. businessfrance-tech.fr

cybersecurity capital, although many entrepreneurs continue to set up in Tel Aviv. Since 2015, Beersheba has become home to the cybersecurity authority's national office, Ben-Gurion University of the Negev which specialises in cybersecurity, the army's cybersecurity centre and the business centre CyberSpark, where a large number of multinationals such as IBM and Dell have established their strategic cybersecurity centres.

In the United States, government agencies are at the heart of the cyber ecosystem. The National Security Agency (NSA) has formed partnerships with American universities. The CIA has its own In-Q-Tel investment fund, which can invest in both American and foreign companies. The Defense Advanced Research Projects Agency (DARPA) is an agency in the U.S. Department of Defense that is responsible for researching and developing new technologies for military use. It was behind the development of many technologies, including IT networks, most notably ARPANET, which later became the internet. Today, DARPA provides financial support to enable the best students in cybersecurity to write their dissertations. The resulting companies are protected from foreign investors by the "Committee on Foreign Investment in the US" (CFIUS)[28]. CFIUS is an interagency committee authorised to review certain transactions involving foreign investment in the United States and certain real estate transactions from foreign nationals, to determine the effect of such transactions on the national security of the United States.

In France, Cyber Campus, a 26,000 square metre tower at La Défense, inaugurated in February 2022, is the result of two years of interaction and discussions between cybersecurity players and the French government. The campus hosts representatives from cybersecurity companies of all sizes, specialised schools, and government services and research institutes, such as INRIA. The goal is to create a favourable environment for technological innovation and to raise the profile of the French cybersecurity sector. Between 1,600 and 1,700 people work on the campus, 30% of those working for large companies and 25% working for government services (National Agency for Information Systems Security, gendarmerie, police or intelligence services, ComCyber military cyber defence).

28. home.treasury.gov

Cybersecurity as an element of industrial policy

For most governments of the world's largest economies, as with technology in general, there is a clear, state-level strategy for cybersecurity. In this area, China and the United States share a policy of technological development within the framework of a national strategic vision. This is vital because the level of investment needed to advance in areas such as artificial intelligence is huge and requires both private firepower from corporate giants capable of investing considerable sums, and a public will to develop and support them. This requires grant schemes for start-ups, public contracts and a very clear development plan for civil and military technological infrastructures. The United States sees technological dominance as a geopolitical weapon. Their geographical location, far from Eurasia, which is home to the bulk of the world's population, means they need to maintain technological dominance, a sector which has become more important than controlling land and sea routes. If we look at demographic trends up to the year 2100[29], Asia's population is set to rise to five billion (from four billion in 2020) and Africa's is set to rise to four billion (from one billion in 2020). These two continents will then represent 80% of the world's population. It is therefore

THESE TWO CONTINENTS (AFRICA AND ASIA) WILL THEN REPRESENT

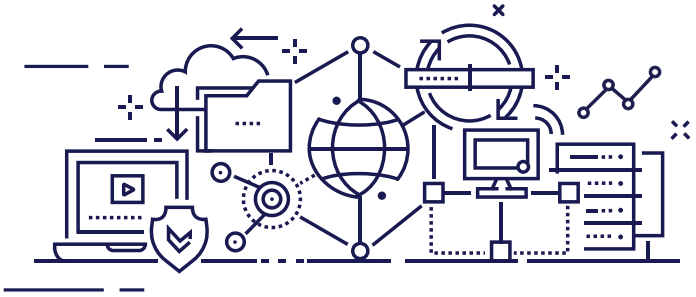
80%

OF THE WORLD'S POPULATION.

29. Tikehau CIO letter – Just about people, June 2021

likely that the Indian Ocean will become the heart of the global economy, as the Atlantic Ocean was in the 20th century and the Pacific has been in the 21st. However, the United States, which borders these last two oceans, does not border the Indian Ocean, which is on the opposite side of the world to North America. To maintain its global economic dominance, the United States will need to be able to project its power far beyond its geographical borders. Technology is therefore key to maintaining its position as a global leader.

For China, the challenge is just as geostrategic as it is domestic: maintaining a hold on its vast population to ensure controlled economic development in a period of rapid urbanisation. In the context of cybersecurity, it is worth taking a moment to discuss the evolution of China's growth model. China's entry into the World Trade Organization in 2001 doubled global labour supply, causing the largest supply shock in economic history. China's numerous, educated and low cost working-age population contributed to making the country the workshop of the world and the number one exporter worldwide, all in the space of a decade. The combination of its significant population size on a global scale, its integration into the global economy acquired under very favourable conditions, and a political regime that maintains absolute control of the economy, allowed China to achieve what no other country has been able to achieve since, and what no other will probably be able to ever again: to move from the status of a poor country in 1980, suffering from underdevelopment and famines, to that of a country set to be the world's leading economy by 2030. State control of the Chinese economy guarantees the success of a growth model based on exports made competitive not only by the cost of its labour, but also by an artificially devalued currency. But since the Chinese population is starting to undergo an enormous demographic turnaround as its population ages, this trend reversal coincides with the rise of China's geopolitical ambitions. These ambitions come hand in hand with the need to change the development model, by imposing its way of thinking on its trading partners in order to build an economic sphere of influence. In order to achieve this, China needs to develop an import economy, and this is just as well, because as the country's population ages, it will no longer be able to remain competitive with an export-centred model. Its foreign exchange reserves are dwindling, and its working-age population is shrinking as a result of ageing accelerated by decades of a one-child policy. Households often have two salaries (the female



employment rate is high) and once the only child has left home, their purchasing power increases to the point that consumption expenditure in absolute terms is set to exceed that of the United States around 2024, making Chinese consumers a major driver of global growth. But in seeking to catch up economically in order to increase gross domestic product per capita, China has sacrificed three elements: environmental considerations which have now put the brakes on its development, its currency independence from the American dollar and its egalitarian communism. From now on, the challenge for China is simple: to restore the balance in these three areas. **Behind the Chinese government's increasingly militant intervention in the technology sector lurks a deliberate decision to shift its focus away from short-term economic growth in favour of other goals: reducing inequality, ensuring social stability and tackling its demographic problem.** The cancellation of Ant Group's initial public offering, the various antitrust proceedings initiated against tech giants who had been in a position to create monopolies, and the severe restrictions imposed on online education have all sent a message to both Chinese businesspeople and markets: China's priority is not entertainment tech or consumer tech, but tech that addresses the priorities of industrial policy. This refers to tech that will guarantee independence from the United States and reduce social inequality. Investors should therefore support sectors favoured by the government. Amongst these, cybersecurity is likely to occupy a prominent place.

The United States and China have therefore made technology and cybersecurity central to their industrial policy. Israel has done the same with remarkable efficiency. Europe has not been as systematic in this area. The two leaders in the field of cybersecurity, the United Kingdom and France, have chosen to adopt public-private partnership policies in this sector, but this is not the case in all European countries. Moreover, following Brexit, France is the only remaining country in the European Union that is in a position to integrate cybersecurity into an industrial policy.

This Sino-American industrial dominance is coupled with Europe's political weakness on the economic front. Between Member States, there is no consensus on the need to implement a genuine industrial policy to foster a European digital industry. Therefore, while France and Germany talk about "digital sovereignty", Northern European countries advocate a much vaguer notion of strategic autonomy and see Europe merely as a market. But despite its internal differences, Europe has laid the foundations for a unified vision of digital space based on a rejection of commercialising personal data and mass surveillance. Beyond these main principles, a variety of measures and legislation have been adopted by the European Union in the digital field, such as GDPR[30] and the "cyber diplomacy toolbox"[31]. Other legal mechanisms are being put together, such as the Digital Services Act or the Data Markets Act. In terms of industrial standards, the Cybersecurity Act, which came into force in 2019, has established a cybersecurity certification framework that applies to all IT products, services and processes. As for the Gaia-X project, this aims to create an interoperability standard facilitating the exchange of data between cloud platforms to develop the "data economy". The crisis in Ukraine will likely lead to strengthening European cohesion in terms of cybersecurity.

The future of Europe will probably involve reindustrialisation and reshoring production, with the aim to strengthen business resilience and create jobs. Reindustrialising means deciding what your priorities are and accepting that you cannot be good at everything. National industry requires a strong demand, either stimulated by public procurement or by changes in corporate purchasing policies which support the development of a framework of local ecosystems. A change in individual behaviours that favour national industry is also part of the equation. The challenge that has arisen in this industrial renaissance is how to also reshape our system, which the crisis has revealed to be running out of steam. The crisis has revived the desire to produce, invent and innovate in Europe. Producing in Europe means providing new outlooks to the region. This means investing in modernisation, "digitalising production processes" and supply chains, but it also entails exposure to cyber risk. For this reason, cybersecurity must be part of industrial policies in the 21st century.

30. General Data Protection Regulation
31. iss.europa.eu

Éléna POINCET
Co-founder and Executive Director
of TEHTRIS

Previously an operational expert in the management and leadership of specialised teams for the French Ministry of the Armed Forces. Elected “2020 IT Personality of the World of IT”, winner of the 2021 “Bold Woman Award” by Veuve Clicquot and the 2022 Digital Women’s Day (JFD) “Margaret” award.

Hyperautomation

for Enhanced Cybersecurity

CYBER THREATS ARE ESCALATING AND BECOMING MORE COMPLEX. THE SPEED OF ATTACKS IS INCREASING AND BEGINNING TO EXCEED OUR HUMAN ABILITY TO PROCESS INFORMATION AND REACT.

Attacks have been found to take as little as 37 minutes, from intrusion to data exfiltration and deploying ransomware on digital assets. When dealing with these unknown threats, information systems teams are powerless if they resort to merely detection for some and human-managed neutralisation for others. Nowadays, traditional tools are no longer sufficient.

IN RESPONSE TO THE THREATS ENCOUNTERED BY ISSMS (INFORMATION SYSTEMS SECURITY MANAGERS), TEHTRIS USES HYPERAUTOMATION TO ADDRESS THIS ISSUE OF IMMEDIACY THANKS TO THE TEHTRIS XDR PLATFORM.

Ever since its conception in 2012, the design of the TEHTRIS XDR Platform has been modelled on Industry 4.0: extensive automation, machine learning and deep learning, all thanks to our Artificial Intelligence module, Cyberia. This approach is orchestrated through our integrated SOAR (Security Orchestration, Automation & Response) tool. As a result, the entire infrastructure is monitored, and unknown threats are detected and neutralised in real time and without any human intervention. Data from the various cybersecurity modules is intelligently correlated to provide full visibility.

HOW DOES THIS WORK IN PRACTICE?

The modules of the TEHTRIS XDR Platform are intelligent sensors which are placed on digital assets that aggregate and analyse all data centrally and provide a holistic view of cybersecurity. These modules come in the form of system sensors – TEHTRIS EDR/EPP/MTD – which are designed to protect computers, servers, phones, tablets, etc., and network sensors – TEHTRIS NTA – which focus on monitoring flows. The TEHTRIS SIEM module makes it possible to centralise, correlate and archive all event log data from the customer environment. TEHTRIS Deceptive Response initially lures and detects attackers. The modules then communicate and interact with each other through the SOAR tool and relay all the data back to the analysts. Cyber surveillance teams can quickly propose risk reduction and mitigation actions. This system is doubly effective since it is self-powering and learns from its findings. In addition, the XDR platform is flexible given that it can accommodate all cybersecurity modules available on the market.

CONCEIVED AND DESIGNED TO SIMPLIFY, CENTRALISE AND ORCHESTRATE, THE TEHTRIS XDR PLATFORM THEREBY ALLOWS ANALYSTS TO FOCUS ON TASKS WITH CONSIDERABLE ADDED VALUE.

To adapt to the ever-changing environment of threat and risk, organisations need flexible and easy-to-operate solutions that save their security staff time, centralise data and optimise cybersecurity without overloading their systems. The future therefore lies in hyperautomation, which is necessary for providing enhanced cybersecurity to protect companies.

IT IS IMPORTANT TO REMEMBER THAT WE WERE THE FIRST TO OFFER THIS TECHNOLOGY AT THE VERY BEGINNING.

The TEHTRIS XDR Platform is now "celebrating" its 10th anniversary and remains the only 100% native European XDR platform capable of detecting and responding to cyber attacks by providing a unified view of all the digital assets of both companies and public authorities.

TEHTRIS IS A COMPANY SPECIALISING IN CYBERSECURITY AND PRODUCES CYBER-DEFENCE SOLUTIONS THAT COMBAT CYBER ESPIONAGE AND CYBER SABOTAGE.

The company was founded in Pessac in 2010 by Éléna Poincet and Laurent Oudot. The TEHTRIS XDR Platform serves every business sector in the world. The hyperautomation of TEHTRIS' solutions is based on artificial intelligence and is designed to automatically detect and neutralise unknown threats in real time and without relying on any human intervention. TEHTRIS raised a record-breaking 20 million euros in Series A funding in December 2020, led by Tikehau Capital.

Cybersecurity as an element of sovereignty

The second industrial revolution came when coal was replaced by oil. Oil is incredibly energy efficient, and this enabled people to produce a greater number of machines that were also more powerful. According to Matthieu Auzanneau in his book on the history of oil, when oil proved to have the remarkable potential to create a scale effect in production, the subjugation of entire societies became superfluous, because it was enough to ensure the support of a few tribal chiefs in order to gain access to oil concessions. The modalities of colonial control then passed from military order to the capitalist one[32]. In the 21st century, data has become the raw material for value creation. Just as most wars in the 20th century can be read through the lens of issues of oil, the conflicts of the 21st century will likely be linked to technology and data. The tensions around Taiwan and its position as a leading producer of semiconductors illustrate this. Data collection and exploitation create economic value in a way that is all the more profitable when the quantities involved are huge.

> IN THE 21ST CENTURY, DATA HAS BECOME THE RAW MATERIAL FOR VALUE CREATION.

Attempts at benchmarking are emerging, which aim to measure the level of state sovereignty in cybersecurity. The Global Cybersecurity Index (GCI), published by the International Telecommunication Union[33], a United Nations agency, measures the cybersecurity maturity of 193 countries around the world. The French company Thales's NCSI[34] provides a more precise assessment of national digital sovereignty, helping each nation to determine where it stands and what it needs to improve in order to achieve its national strategy objectives for education, training, research, improving business cyber maturity, sovereign technology and government capabilities[35].

32. Black Gold, the Great History of Oil, Matthieu Auzanneau, 2015
33. International Telecommunication Union – ITU
34. National Cyber Sovereignty Index™
35. thalesgroup.com

But in the realm of technology, the United States and China are increasing their lead over other nations, to the point of threatening the sovereignty of other countries. Both countries benefit from the size of their "domestic markets" for data, and they are also homogeneous in terms of language, regulation and legislation. Therefore, the world's three leading economic blocs should, in theory, emerge as clearly dominant in this industry. However, Europe suffers from several structural weaknesses. The first is the absence of a homogeneous European domestic market, which likely explains why there are no European technology giants comparable to the American and Chinese ones. There is still a big gap between SAP and Dassault Systèmes in Europe, and GAFAM in the United States or BATX (Baidu, Alibaba, Tencent and Xiaomi) in China. Europe has also chosen to protect consumers by imposing strict regulations on the use of personal data in the form of the General Data Protection Regulation[36]. This side of the issue is significant because it likely determines which bloc will be able to take the leadership in the field of artificial intelligence. In this respect, China probably has a considerable advantage, namely its model of "controlled democracy". The implicit contract between the Chinese Communist Party and the people since China's entry into the World Trade Organization is relatively clear: Chinese citizens accept that they have a stable regime, and in exchange, the party offers an increased standard of living and restores China's leadership position in the world, which is highly important to the Chinese people. The greater tolerance of personal data use is a considerable competitive advantage that China possesses in the race for technological dominance.

If we add to this the quality of the education system, the number of engineers graduating each year, and the power of industrial policy and public–private partnerships, we can understand why China and the United States are ahead in the technology race. In cloud computing for example, ten or so players, mainly Americans, have a 77% share of the world market. The first company in Europe, OVHcloud, only has around a 1% market share. The findings are the same in the electronic components industry: Europe produces merely 9% of the world's semiconductors, a market largely dominated by Taiwan. As a result, American and Chinese companies dominate the data industry (storage, analysis, trade), and this poses a definite challenge to the sovereignty of other countries. There is a high risk that tensions between China and Taiwan will cause supply disruptions in the semiconductor industry and consequently to global industry as a whole. In 2013, the WikiLeaks affair made it clear to Europe how important digital sovereignty really was.

36. GDPR is an EU regulation serving as the reference text for the protection of personal data. It reinforces and unifies data protection for individuals within the European Union. This regulation was definitively adopted by the European Parliament on 27 April 2016

China and the United States are therefore on track to capture an increasingly significant proportion of global wealth creation, not only thanks to a virtuous circle of value creation for entrepreneurs who then reinvest in local infrastructure, but also thanks to companies which meet global needs and therefore tend to form monopolies at the expense of local players. PricewaterhouseCoopers estimates that the spread of artificial intelligence will thereby increase global GDP by $15.7 trillion between 2020 and 2030. China alone would obtain nearly $7 trillion of this added value[37]. Creating economic value is therefore concentrated in tech, and the weight of this sector in the global economy is so significant that it shuffles the balance of power and threatens the sovereignty of every country in the world. In this regard, it is unsurprising that the two countries in the leadership position are asking other countries and their companies to "pick a side".

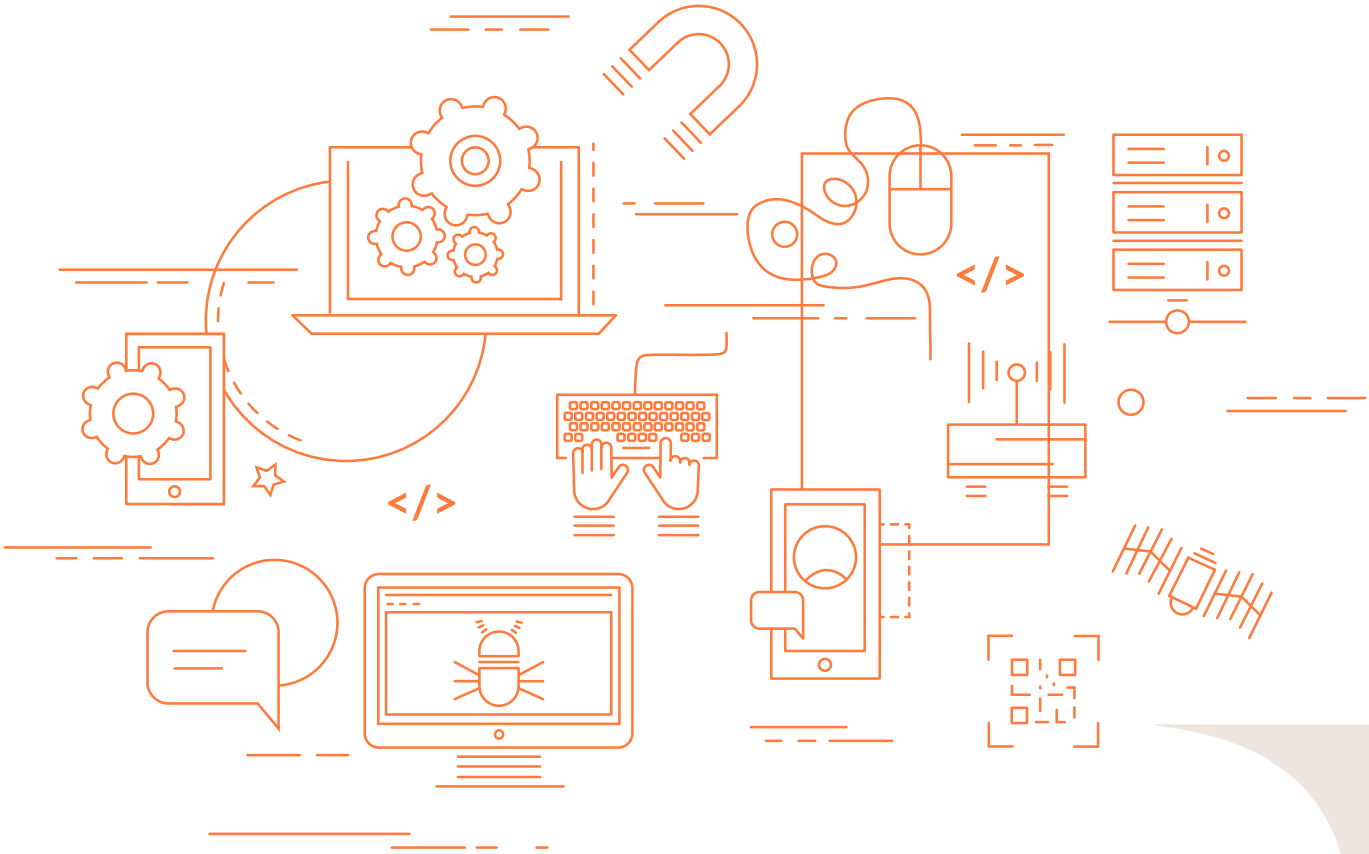
> THE SPREAD OF ARTIFICIAL INTELLIGENCE WILL THEREBY INCREASE GLOBAL GDP BY $15.7 TRILLION BETWEEN 2020 AND 2030.

> CHINA AND THE UNITED STATES ARE THEREFORE ON TRACK TO CAPTURE AN INCREASINGLY SIGNIFICANT PROPORTION OF GLOBAL WEALTH CREATION.

Consequently, at the 2021 NATO summit in Brussels, Allies endorsed a new Comprehensive Cyber Defence Policy, which supports NATO's core tasks as well as its overall deterrence and defence posture, which further strengthens the resilience of the Alliance. **This trend is likely to not only accentuate tensions between these two countries, but also to profoundly change their relationship with other countries, particularly in the field of digital sovereignty.**

In this regard, it is likely that all companies in the sector will need to examine the relationship they have with nation states on issues of geostrategy. To what extent can a company's nationality ensure that they act in the interest of their country of origin? How much will their activities in this field threaten their ability to develop beyond their country's borders? What

37. Sizing the prize – PwC, Anand Rao, Gerard Verweij, June 2017



will the balance of power look like between companies that are capable of investing massively in strategic programmes on the one hand, and governments that must consider their ability to cause social harm on the other?

Here, it is interesting to consider the alliance between the American company Google and the French company Thales. In October 2021, the two companies announced a joint venture to offer a "sovereign cloud" service in France. It is one of only a few transnational cooperation initiatives on the issue of digital sovereignty to date. Its aim is to enable French companies and public institutions to migrate their critical applications and sensitive data, benefiting from a cloud service package operated by a company under French law. This company, with Thales as the majority stakeholder, is hosted in France within an infrastructure that is separate from the Google Cloud platform, and whose network and servers will be controlled and operated by the new entity. The new company will provide customer support and service security locally. This primarily includes identity management, data encryption, administration and supervision.

Saving democracies and debate of ideas

60% of the world has access to the internet. This makes it possible for this substantially large number of people not only to communicate with other people around the world on an unprecedented scale, but also to access an enormous amount of information. In less open societies, authorities used to assume the role of social protector, imposing the sovereign power of the state. The tacit democratic pact documented by the Greeks and the Romans, whereby a population would submit to a public authority in exchange for protection, has now been undermined by access to an abundance of information. At a time when democracies have to deal with the problems posed by attempts to manipulate information, the security of data and access to information appears key to defending the democratic model. Indeed, unlimited access to information actually makes expressing opinions more difficult. The globalisation of information has impoverished debates of ideas and the number of subjects open to debate has diminished, in proportion to the sensitivities of particular groups of people who think the same way, even if they are on opposite sides of the world. It is much easier to create misinformation, harass people on social media or destabilise society by manipulating information nowadays than it was when information

60%

OF THE WORLD HAS ACCESS TO THE INTERNET

came exclusively from the press or television. The fact that deepfakes appear so real is an example of this[38]. These phenomena pose a threat to democratic regimes. Furthermore, when foreign powers interfere in an election by orchestrating a disinformation campaign, this can influence its outcome. The democratic model appears vulnerable and must be protected, partly by strong cybersecurity legislation, but above all by sophisticated and effective technical defence capabilities, or even by a force of cyber deterrence.

Even more insidious is data accumulation, not just on consumer habits, but also on what attracts people's attention when surfing the web. This creates filter bubbles that threaten the kind of public debate which is vital for democracy. It is likely that artificial intelligence can detect cognitive biases and influence decision-making based on those inferences. By exploiting the cognitive bias that encourages people to favour and accept information that confirms their own point of view, these companies trap consumers in what Eli Pariser[39] calls a "filter bubble", i.e., a mechanism that recommends products or content which fulfil the preferences, tastes or desires identified by the algorithm. People can choose their own version of the truth and have their views and beliefs reinforced by exposure to opinions that confirm their own, and this risks fragmenting society in a way that causes dialogue to break down. **In this area, cybersecurity alone is not enough to preserve the democratic model, although it is necessary. There is obviously a limit to what cybersecurity can achieve, but protecting against attempts to falsify data, manipulate votes or spread false information is part of the arsenal needed to defend national sovereignty. This is the case for democracies as well as other regimes.**

To maintain its integrity, cyberspace must remain a space of freedom and interaction. Cybersecurity now forms part of the power strategies and power relations that govern international relations. The Paris Call for trust and security in cyberspace[40], a French initiative in the field of cyberdiplomacy which sets out 9 main principles, has been signed by 81 countries. Since 2004, the United Nations has been working on issues related to security and stability in cyberspace, with the aim of preventing cyberspace from becoming a zone of lawlessness. It is vital that international law applies to cyberspace. The French government website[41] states that the emphasis is now on helping the least developed countries to increase their overall level of cybersecurity in areas such as protecting telecommunications infrastructures or training their workforces. To contribute to these objectives, France, along with 53 other countries and the European Union, is pushing for a United Nations Programme of Action on cybersecurity to be put in place.

38. fr.wikipedia.org
39. Eli Pariser – The Filter Bubble, What the Internet is Hiding from You, 2011
40. pariscall.international
41. diplomatie.gouv.fr

Cybersecurity as a military tool and a form of state espionage

Past cyber attacks led by state actors have primarily been carried out in order to gather information rather than to destroy equipment or data. It is therefore difficult to predict the potential impact of a cyberwar between governments. A few studies have attempted to model the potential economic costs of cyber attacks which are technologically possible on US critical infrastructure[42]. A study by the New York Fed estimates that a successful attack on one of the largest US banks could disrupt between 5% and 35% of daily payments. A study by Lloyds estimated that an extreme attack on the Northeast US power grid could cause between $250 million and $1 billion worth of damage.

In terms of cyber threats, as early as 2011, during the International Cybersecurity Forum, the Vice-President of the European Commission, Margarítis Schinás, warned that Europe is in a "critical situation" as a result of an increase in cyber attacks. During this same event, the French Minister of Defence, Florence Parly, announced the recruitment of "770 more cyber warriors, set to reach 5,000 in 2025 within the French armed forces, the General Directorate of Armaments (DGA) and the French foreign intelligence agency DGSE." In June 2019, in a hearing at the French Senate, General Lecointre, former Chief of Staff of the French armed forces, acknowledged the use of cyber weapons: "Regarding external operations and the danger to our forces, when the enemy has a capacity for cyberwarfare, we use cyber weapons just like weapons would be used on the battlefield. We know how to disrupt an enemy, locate them and deal with them. We often use cyber weapons as a tool in combat. This requires resources and specialists, but it gives us a very clear advantage in the Sahel or the Levant."

The Russia-Ukraine crisis shows how cyberwarfare has come to complement the conventional military arsenal in disrupting or even neutralising the enemy's capabilities. As of 14 January 2022,

42. The economic impact of cyber attacks – Goldman Sachs US economics analyst, 7 March 2022

the military news site Opex 360 reported that Ukraine was the object of a cyber attack that targeted around fifteen government websites, including the Ministry of Foreign Affairs. Before it became inaccessible, it had posted a statement urging Ukrainians to "prepare for the worst" because all their personal data had been "uploaded onto the public network"[43]. The use of various new strains of Wiper, sabotage malware capable of destroying any data or systems in its path, was detected[44]. From the very start of the conflict, groups of hackers began to get involved on both sides. Notorious hacker collective Anonymous claimed it was behind a distributed denial-of-service (DDoS) attack that took down Russian news site RT and hacked into other Russian TV channels to broadcast the Ukrainian national anthem. Some hacker groups like Conti, The Red Bandits, SandWorm and the Belarusian UNC1151, on the other hand, have sided with Russia. In response, Conti was hit with a massive internal data leak (in which 60,000 internal messages, including its source code, were made public). On 24 February 2022, the Ukrainian government called for volunteers from the country's underground hacking community to help protect critical infrastructure and conduct cyber espionage missions against Russian troops. On 26 February 2022, Ukrainian Deputy Prime Minister Mykhailo Fedorov announced the creation of the "volunteer IT army".

At the same time, Russia also reportedly stepped up efforts to exploit its own internet, with the intention of cutting it off from the global infrastructure.

Overall, the impact of these cyber attacks has been limited, but there is a risk of collateral damage to international cyberspace. For example, on 28 February 2022, the American satellite communications company Viasat announced that it was investigating a cyber attack that caused a partial outage of its residential broadband network that covers Europe, including Ukraine. Terrestrial modems providing connectivity between satellites and users were compromised. This attack caused significant collateral damage, particularly to the remote control of wind turbine networks, which amounts to a production capacity of 11 gigawatts in central Europe.

The Russia-Ukraine crisis therefore demonstrates that cyberwarfare now makes up an integral part of new military conflicts. Therefore, it is unsurprising that the United States wants to create a "cyber NATO"[45].

43. opex360.com
44. cert.ssi.gouv.fr
45. nato.int

Cybersecurity lies at the heart of the new industrial revolution, which arose out of data use and artificial intelligence. In the 21st century, it is a key area in every country's industrial policy. However, the scope of cyber issues extends beyond simple defensive and sovereignty considerations.

To ensure its long-term durability and address its extraordinary vulnerability, as highlighted first by the COVID-19 crisis and more recently by the Russia–Ukraine crisis, the global economy must completely reinvent its growth model and become more resilient. Like the transition to renewable energy, cybersecurity is part of the solution to building a more resilient economy. A more sustainable economy requires technology that both restores trust between economic actors and strengthens the resilience and efficiency of productive capacities. Strengthening the quality and traceability of goods and services, preserving jobs through good ecosystem resilience and using technology to recreate social ties requires massive investments in cybersecurity. Without cybersecurity, there can be no trust. And trust creates economic value.

Cybersecurity is therefore at the heart of the industrial data revolution, which brings with it considerable environmental, social and governance challenges. For the first time in human history, the long-term interests of the entire world population are aligned. Cyber risk has probably created one of the most significant investment opportunities for the next few decades.

MAY 2022

CIO letter

TIKEHAU CAPITAL

32, rue de Monceau 75008 Paris - FRANCE

Tél. : +33 (0)1 53 59 05 00
Fax : +33 (0)1 53 59 05 20