MODERN CYBERSECURITY: NEW ERA, NEW STRATEGIES

November 2024

isms forum

Modern Cybersecurity: New Era, New Strategies

Sergio Álvarez-Teleña [1 2] **Marta Díez-Fernández** [2] **ISMS Forum** [3]

Abstract

This essay *(a)* overviews the literature of Algorithmization to provide the reader with a solid background to discuss Modern Cybersecurity; *(b)* introduces new high-priority risks to be considered by both business and cybersecurity teams; *(c)* roots the resourcing of cybersecurity on the hybridization between business, compliance and cybersecurity; *(d)* discovers novel capacities unlocked by an algorithmic-native platform to harmoniously orchestrate both business and cybersecurity; *(e)* seeds the future of the business and its continuity-at-risk on tactical technology; and *(f)* motivates a new breed of hands-on research in collaboration between companies and research centers upon platforms that follow the Three-Layer Company model.

1. Introduction

This paper examines how to make informed decisions in the face of an increasingly unknown and evolving environment on cybersecurity. The rapid evolution of the companies into algorithm-driven entities serves as the trigger for this initial essay on cybersecurity[1]. Before delving into specific details and case studies in subsequent papers, this document aims to take a step back, offering a broader perspective on this new era. Our goal is to help the reader understand the overarching landscape, enabling them to see the forest rather than getting lost among the trees.

In the second chapter, we explore the existing literature on measuring the impact of cyber insecurity, a traditional method used to allocate defense budgets. We begin by analyzing national-level survey data and questioning its continued relevance. From there, we pivot away from historical data, shifting our focus toward advanced transformation literature to prioritize plausible dynamics - and therefore plausible data over past data. Readers who are less interested in the intricacies behind the challenge of measuring the impact of cybersecurity can step directly into chapter three.

Chapter three offers the first zoom-out on advanced transformation of the paper, questioning whether AI serves as the foundational element of new infrastructures or it is merely the cherry on top. To approach this, we split the companies into two factories: the traditional blue-collar and a new one, white-collar.

The fourth chapter zooms-out again, addressing the fact that white-collar factories will broadly exist in an economic equilibrium due to needs for efficiency and productivity in competition. For that we distribute a company's nature into three layers: Core I (infrastructure), Core II (all departments in one platform) and Orbit (idiosyncrasy that leads to differentiation). This approach allows senior management to precisely control shifts in the company's supply curve, guiding its strategic efforts to dominate and expand within its market.

Chapter five, provides the last zoom-out on advanced transformation of the paper. We put the focus on a necessary condition for the former two - business continuity. As attackers become more professional through Algorithmization, business discontinuity becomes a major issue for all departments within a company. Thus, we will be witnessing a hybridization of the decision making process between business, cybersecurity and compliance. As, given the fact that technology budgets at companies are constrained by profitability and past data is not good enough to forecast the impact of CISOs' budgets, as explained in chapter 2, it is crucial in the future of companies to start leveraging the upside of hybridization - largely, the budget sharing. Companies need to take a step back on how they look at their technology legacies so that the budget is properly agreed across the three and hence, optimized for the new

[1] Department of Computer Science, University College London, UK [2] SciTheWorld, Spain [3] ISMS Forum, Spain. Correspondence to: Sergio Álvarez-Teleña <sergio@scitheworld.com>, Marta Díez-Fernández <marta@scitheworld.com>, ISMS Forum <info@ismsforum.es>.

[1] Funded by the International Information Security Community (ISMS Forum).

era. More interestingly, we introduce a set of new risks and new mitigations in an algorithmic-driven world - Tactical Technology, CNE's Game Theory and market price manipulation are examples of what the reader will be exposed to.

The final chapter offers conclusions and suggests areas for future work.

2. Background: Only Action Creates Traction

We begin this chapter reviewing the existing literature on measuring the impact of cybersecurity, with the aim of identifying the challenges and limitations of using it as a key performance indicator (KPI) for guiding corporate cybersecurity budgeting decisions. This analysis sets the stage for understanding the complexities involved in aligning cybersecurity investments with measurable outcomes. Subsequently, we present a thorough overview of recent research on advanced digital transformation, laying the groundwork for a more in-depth exploration of this topic in the following sections of the paper.

2.1. Not Everything can be Measured: KPIs, a Burden in Transformation

To assist organizations in determining the appropriate levels of investment necessary to address the escalating risks associated with cybersecurity, we initially considered conducting a national-level survey aimed at estimating potential costs on a countrywide scale. The primary rationale for this approach was to quantify these costs as a percentage of GDP, thereby providing standardized benchmarks that companies could use to align their defense budget to their profit and loss statements (P&L). This methodology was intended to enable informed decision-making regarding cybersecurity investments, ensuring that companies are adequately prepared to mitigate emerging threats.

Upon a thorough review of existing public documents related to previous efforts in this domain, [1], [2], [3], [4]... several significant limitations became apparent:

1. **Insufficient publicly available data on cyber capabilities**: The availability of data on cyber capabilities, both classified and non-classified, is significantly limited. This scarcity creates substantial challenges in making accurate cross-country comparisons, as the lack of comprehensive and consistent data hampers the ability to assess and benchmark cybersecurity strength and readiness across different nations.
2. **Limited availability of English-language information**: For some countries, crucial information is not readily available in English, further complicating efforts to obtain reliable and comparable data across different regions.
3. **Lack of data on cyberspace proxies**: There is a significant scarcity of data concerning proxies in cyberspace - entities or intermediaries that operate on behalf of other actors, often masking the true source of cyber activities. This lack of information poses a critical challenge, as it severely limits the ability to fully comprehend the scope, scale, and complexity of cyber operations. Without detailed data on these proxies, it becomes difficult to accurately attribute cyberattacks, understand the networks and strategies employed by cybercriminals, and assess the broader impact on global cybersecurity. This gap in knowledge also complicates efforts to develop effective defense mechanisms and international policies, as the hidden nature of proxy activities obscures the true capabilities and intentions of both state and non-state actors in cyberspace.
4. **Lack of homogeneous data**:
   - *Across Countries*: The availability and quality of data on cybersecurity vary significantly from one country to another. This inconsistency stems from differences in reporting standards, data collection methodologies, and the level of transparency regarding cyber capabilities and incidents. As a result, making direct comparisons between countries is challenging, as the data may not be directly comparable due to these discrepancies. This variability undermines the ability to develop a cohesive understanding of global cybersecurity trends and hinders international cooperation in addressing cyber threats.
   - *Across Sectors*: Data inconsistency is also prevalent across different economic sectors. Industries such as finance, healthcare, and energy may have varying levels of data availability and reporting practices, influenced by factors such as regulatory requirements, sector-specific risks, and the adoption of cybersecurity measures. This lack of uniformity makes it difficult to conduct reliable sector-specific analyses, as the data may not accurately reflect the true cybersecurity posture or risks within each sector. Consequently, this variability complicates efforts to benchmark performance, identify vulnerabilities, and allocate resources effectively across different industries.
   - *Over Time*: The uniformity of data collected over different years is often lacking, making it difficult to conduct longitudinal studies or identify trends

over time. Changes in data collection methods, evolving cybersecurity threats, and shifts in reporting practices contribute to this inconsistency. As a result, efforts to track the progress of cybersecurity measures, evaluate the effectiveness of policies, or forecast future trends are hindered by the lack of a stable and comparable data set. This temporal variability poses a significant challenge for researchers and policymakers attempting to assess long-term developments in the field of cybersecurity.

5. **Unreliable survey data**: Surveys are a common tool for gathering data on cybersecurity capabilities and activities; however, the reliability of this data is frequently compromised by strategic factors. Countries may intentionally obscure or misrepresent their true cyber capabilities and intentions to protect national security interests. This deliberate concealment is often motivated by a desire to maintain a strategic advantage, avoid revealing vulnerabilities, or mislead potential adversaries. As a result, the data collected through surveys may not accurately reflect the actual state of a country's cybersecurity infrastructure, leading to significant underrepresentation or misrepresentation in global indices and studies. For example, in [4], it has been suspected that Israel might be significantly underranked due to its strategic choice to obscure its cyber capabilities. This underreporting can distort global rankings and analyses, leading to an inaccurate portrayal of a country's cyber power relative to others. Such strategic behavior complicates efforts to create accurate and comprehensive assessments of global cybersecurity, as the data is often incomplete or misleading due to these intentional omissions. This issue underscores the broader challenge of relying on self-reported data in a domain where secrecy and strategic deception are commonplace.

6. **Methodology**: Most of the papers claim to follow a rigorous methodology and then they highlight verifying their analysis using NLPs, which as seen in [5] is not the best practice. A combination of domain expertise, robust statistical methods, and careful consideration of context-specific factors should guide the validation process. Therefore, best practices in cybersecurity research should involve a more holistic approach to verification, ensuring that the methodologies used are both appropriate and effective for the specific challenges of the field.

7. **Inconsistency across studies**: Despite the variety of existing studies, most are based on different measures and tools, such as annual costs, sector-specific costs, or costs per attack. This diversity in measurement approaches leads to significant variability in the results, often resulting in inconsistent estimates and forecasts that complicate efforts to draw reliable comparisons or conclusions across different contexts. For instance, one study might focus on the annual financial impact of cyberattacks on large corporations, while another might measure the average cost per incident across various sectors. The lack of standardized metrics means that these studies are often not directly comparable, making it difficult to aggregate data or identify broader trends. This inconsistency is further exacerbated by the differences in how data is collected, reported, and analyzed across studies. Some research may rely on self-reported data from companies, which can be subject to bias or underreporting, while others might use proprietary databases or third-party reports that are not universally accessible or verified. Additionally, the methodologies employed to calculate costs - whether through surveys, econometric models, or simulations - can vary widely, leading to discrepancies in the estimated impact of similar cyber events. The fragmented nature of these studies also poses challenges for policymakers, industry leaders, and researchers who seek to understand the full scope of global cyber risk. Without a unified approach to measurement, it becomes difficult to develop effective strategies for mitigating these risks or to allocate resources appropriately. The lack of consistency can also hinder international collaboration, as countries and organizations may base their cybersecurity policies on different sets of data, leading to a disjointed global response to cyber threats. Moreover, the focus on specific costs - such as those associated with individual attacks or sector-specific impacts - often overlooks the broader, systemic risks posed by cyber threats. These broader risks, which can include disruptions to critical infrastructure, loss of intellectual property, and long-term economic damage, are harder to quantify but are no less important. The current approaches may fail to capture these dimensions, leading to an incomplete understanding of the true cost of cyber risk. In summary, the diversity in measurement approaches within existing studies highlights the significant challenges in producing comparable and consistent figures in the context of global cyber risk assessment. This lack of standardization not only complicates the comparison of results across different studies but also limits the ability to form a comprehensive picture of the global cyber risk landscape, thereby hindering efforts to develop coordinated and effective responses to these increasingly complex threats.

8. **Emerging dynamics of new risks**: Additionally, the new dynamics associated with emerging risks were

not adequately identified in the existing research, highlighting a significant gap in understanding and addressing the evolving nature of cyber threats. As companies increasingly adopt advanced technologies, they expose themselves to a broader spectrum of risks. The integration of digital technologies across all aspects of business operations has created new vulnerabilities, particularly as organizations transition to cloud computing, the Internet of Things (IoT), and artificial intelligence (AI). These technologies, while offering tremendous benefits, also expand the attack surface, providing cybercriminals with more opportunities to exploit weaknesses. Furthermore, the sophistication of attackers has grown in parallel with technological advancements. Cyber adversaries are now capable of leveraging state-of-the-art algorithmic innovations. The traditional defenses that companies have relied upon may no longer be sufficient to counter these advanced threats, leading to an urgent need for organizations to reassess and strengthen their cybersecurity strategies. We found this issue particularly concerning, as it indicates that current risk assessments may be significantly underestimating the potential impact of these new threats. The failure to fully account for the dynamic nature of cyber risks means that companies may be inadequately prepared for the challenges that lie ahead. This inadequacy could result in severe financial losses, reputational damage, and disruptions to business continuity. Recognizing these limitations, we decided to shift from a predominantly statistical approach to a more microeconomic one, focusing on developing well-founded reasoning within the field. By adopting this approach, we aim to better justify the key changes that may be necessary for companies to adapt to the evolving cyber threat environment. This involves not only reassessing current security measures but also considering broader organizational changes, such as restructuring cybersecurity governance, investing in advanced threat detection and response capabilities, and fostering a culture of continuous learning and adaptation within the workforce. Ultimately, this more nuanced understanding will help companies to make informed decisions about where to allocate resources, how to prioritize different risks, and what strategies to implement to safeguard their operations in an increasingly complex digital landscape.

After all these intricacies, the wonder was: when data cannot be leveraged to make informed decisions, what can be done?.

2.2. Literature on Advanced Transformation: a Novel, Deep Discipline

Economists have been dealing with data-driven and theory-driven modeling for a number of years already. The former led to Econometrics, the origin of nowadays Data Science, and the latter, more relevant in this paper, to Microeconomics and Macroeconomics modeling.

We won't create a model to justify with precision how much each company needs to spend in cyber security. The dynamics within the corporate world and that of the attackers are changing so dramatically upon their advanced Digitalization that it is too early to create such a model. Instead, at this stage, we will be identifying the inputs that would be most significant for the model - without shaping it any further - so that the CISO can decide whether to remain pegged to the past data or to take other communication strategies with the senior manager to address emerging cybersecurity needs.

First, it is essential to thoroughly understand the role of AI and the associated risks. The involvement of AI in transformative processes often leads to the spread of half-truths, frequently propagated by individuals with limited academic credentials and driven by viral marketing tactics. To address this widespread confusion, we have pioneered a new discipline over the past decade: Algorithmization. This discipline redefines Digital Transformation by emphasizing efficiency and productivity, marking an evolution beyond mere Digitalization. Algorithmization represents a shift from companies being data-driven to becoming model-driven, operating according to advanced protocols. These models can be defined mathematically (as in statistics), developed through trial-and-error approaches (as in computational statistics or AI), or based on heuristic rules proposed by experts. As this transformation extends across all departments, the company itself essentially becomes an algorithm. This shift not only introduces new vulnerabilities but also presents novel opportunities for developing defense strategies.

The foundational technology underpinning this shift was meticulously developed and articulated in [6]. The pivotal role of senior management in navigating this shift was thoroughly examined in [7] and [8], while the subtle distinction between applied science and the misapplication of scientific principles, or *science applied*, was critically analyzed in [9]. Additionally, the innovative approach of exerting influence over nations by compromising not only their companies but also their corporate boards was a groundbreaking concept introduced for NATO in [10]. Further cutting-edge examples were provided in [11], [12], and [13],[14],[15]. Lastly, the comprehensive integration of

Algorithmization with Artificial Super Intelligence (ASI) was explored in depth in [5]. This analysis highlighted the symbiotic relationship between these concepts, illustrating that ASI is unlocked through the Algorithmization of departments - achieved by aggregating Artificial Narrow Intelligences (ANIs) - when efficiency and productivity are the primary drivers. This intersection represents a new economic equilibrium that will increasingly shape corporate behavior and, more significantly, the risks associated with it in the future.

2.3. Conclusion

While it is possible to invest time and resources in analyzing past cybersecurity impacts, the reality is that even if such an analysis were straightforward - which it is not - it would be of limited significance from a dynamic perspective. This is because nearly all sectors are undergoing fundamental transformations toward Digitalization, rendering historical data less relevant in the context of rapidly evolving digital landscapes.

The remainder of the paper delves into deep insights about the Algorithmization of attackers and defenders that could be crucial in defining new dimensions of risks, as well as identifying effective mitigations and assessing their potential impacts.

3. AI is a Minor Thing: White Collar Factories as the Real Deal

AI is a lever to unlock transformation in a company but it should be far from being itself the target - a common error that we have witnessed across industries for the last years. In fact, confusing AI with algorithmics, being a subset of the latter, generates not only confusion but undesired legacies.

The Algorithmization of companies refers to the transformation of their departments into operational units that harness scientific methods while maintaining a clear emphasis on professional expertise over purely theoretical or scientific assumptions. A common pitfall, as illustrated in [9], is the misinterpretation of *Applied Science* as *Science Applied*, often resulting in partial solutions that fail to generate significant impact within the organization. To achieve meaningful outcomes the role of science must be appropriately minimized, and that requires judgement across the three: science, technology and business - a very scarce one as the three must be overlapped in the knowledge of one person, the leader, not merely combined in a team.

In this chapter, we outline the reasons behind the growing intensity of the hype surrounding AI. The complexity of advanced transformations, which will significantly shift priorities in cybersecurity, requires not just a single broad perspective, but a series of three comprehensive zoom-outs. This chapter serves as the first in that series, offering an essential foundation for understanding the broader implications of these transformative intricacies.

3.1. Blue Collar Factories: Production is already an Algorithm

Since the introduction of the T-Model in Henry Ford's factories, companies have progressively gained control over time, costs, and quality through the employment of blue-collar workers. The traditional craftsmanship approach was replaced by a meticulously organized system in which less-skilled, more easily replaceable workers were positioned around machines to manage the entire production process. These workers adapted their roles systematically to the sequence of machines, as well as to the machines' operational legacies throughout the factory. In this sense, the factory itself operates as an algorithm, where humans and machines converge - though in this case, the machines are augmented by human labor.

It is important to note that the algorithm governing factory operations is not derived from a self-learning model but is instead designed heuristically by engineers in collaboration with business experts, tailored specifically to the needs of the company. As a result, this algorithm is unlikely to be mathematically optimal, yet *good-enough* in terms of efficiency and productivity to enable the company to remain competitive in the market.

3.2. White Collar Factories: the Offices are the Still-Pending Algorithmization

As companies increasingly adopt similar types of machinery, their production processes have become more standardized and less of a competitive advantage. Consequently, the focus of innovation has shifted from the factory floor to the white-collar sector, driven by the digital transformation movement.

In this context, AI has taken center stage, dominating the narrative around Digitalization and absorbing a substantial portion of corporate innovation budgets. However, it is essential to recognize that AI is only one component within a broader and more fundamental transformation

- one that does not always require AI at every stage. Companies are evolving into fully algorithmic entities, essentially becoming *white-collar factories*, where strategic, operational, and decision-making processes are distilled into formulas. This transformation signals a profound change in how businesses function, as these algorithmic frameworks encapsulate the core operations of the company. As such, these formulas represent the new intellectual property of the corporate world and must be protected with an unprecedented level of diligence, marking a significant shift in the demands of corporate governance.

3.3. Businesses Standardization: Cornered to NPCs (Meaningless Agents)

The way companies have been building their technology infrastructure has been far from optimal. Technology providers often compel their clients to adapt to the providers' own legacy systems, which are designed to scale across multiple clients by offering standardized services. These providers usually operate as part of an oligopoly, meaning that most companies' tech stacks are just slight variations of one another. Moreover, the consultants linking these platforms also belong to an oligopoly, and to scale their services, they push for further standardization across clients.

As a result, companies within a sector are pushed into a state of perfect competition, lacking any meaningful competitive advantage over their peers. This creates a significant business risk, stemming from the prioritization of fragmented decisions over holistic, orchestrated strategies that align technology with both short - and long-term business goals.

Furthermore, this standardization increases vulnerability to cyberattacks. The more similar the platforms, the more attractive and profitable it becomes for hackers to target them. Therefore, evolving technology in a more proprietary and differentiated manner has become an urgent need - *standardization risk* is one that has to be properly explored going forward as it brings risks from a new breed of competitors, from providers to other sectors.

3.4. Conclusion

As companies advance in their digital transformation, they naturally evolve into end-to-end algorithms, spanning both production and office environments. This fundamental shift in their operational structure places increased pressure on the role of cybersecurity, elevating its importance at both the Board and CISO levels. The algorithmic nature of these organizations heightens vulnerabilities, making the protection of data, processes, and intellectual property more critical than ever. Cybersecurity must now adapt to safeguard not only traditional assets but also the algorithmic frameworks that underpin the entire business, requiring strategic oversight and more robust governance at the highest levels.

In the limit, companies must now not only defend themselves against bold cyberattacks but also contend with more subtle, business-oriented risks. For example, standardization risk since they face the challenge of safeguarding against technology suppliers who, intentionally or not, act as *platform hackers* by imposing inefficient architectural designs. Such designs can lock companies into unfavorable systems, reducing their agility and competitiveness. Additionally, companies must address the risk of major competitors leveraging these inefficiencies to dominate the market. This expanding threat landscape requires cybersecurity to evolve beyond traditional defense mechanisms, incorporating a more strategic approach to protect the broader business dimensions of the company.

4. Shifting the Supply Curve: Efficiency & Productivity, the Winner Tandem

If another step backwards is taken to zoom-out again one realizes that, in spite of its relevance, Algorithmization is not an end goal but rather a strategic tool aimed at driving efficiency and productivity to new heights.

This chapter sheds light on the current state-of-the-art technology available to accomplish such a novel approach. Thus, it is intended to provide the reader with a solid base before entering into its implications in cybersecurity.

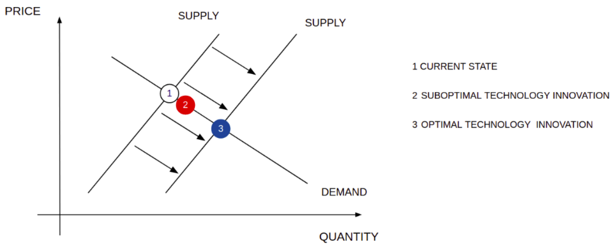


Figure 1. Supply shift with an innovation in the technology of a company: it is not enough to move it but to move it maximally instead and, ideally, over time. Source: [6]

4.1. Extreme Efficiency: the Three-Layer Companies

Those companies that are fully algorithmized - upon blue and white-collar factories - are the ones that can unlock the highest efficiency levels of their industries[2].

We refer to these companies as *on-platform organizations* and they are structured in three distinct layers:

1. **Core I:** the software architecture - federated as in Data MAPs (see [6]).
2. **Core II:** the software apps for the different departments - algorithmic native.
3. **Orbit:** the idiosyncratic fine tune of Core II seeking differentiation - proprietary advances.

They are all thoroughly described in [8] but we will highlight their main characteristics below so that the reader builds a solid background towards the final discussion on modern cybersecurity.

4.2. Core I: Federation

This deep tech layer represents the core of disruption - it's the catalyst that enables everything algorithmic within a company. After publishing its thorough theory in [6], SciTheWorld developed the first instance of such an approach by leveraging algorithmic trading technology. The logic is straightforward: if this technology can successfully manage some of the most intricate strategies across various sectors, then, when properly designed, it should be equally capable of universally handling the strategic needs of other departments within a company. In relation to the focus of this paper, this innovation specifically enables:

- **Algorithmic businesses:** in a way where the departments share backend technology so that its maintenance and improvements are synergistically managed.
- **Algorithmic cybersecurity:** as the technology is spreaded across nodes regardless of the servers they are on, it can leverage its new nature to unlock new strategies for hardware and software management, protection, etc.
- **Algorithmic compliance:** breaking down complex algorithms into nodes makes it easier to enforce and track compliance by design - leading to a novel capacity to discount, real time, the consequences of global regulation.

Note that the three of them can thereon be merged natively. The more effort the company puts into them the more competitive advantages it can unlock. There are a myriad of examples such as:

- **Rotation resilience:** in an era characterized by frequent movement of tech-savvy talent between companies, maintaining a federated system is essential for safeguarding intellectual property and facilitating rapid replacement in key roles. This approach ensures continuity and mitigates risks associated with employee turnover.
- **Cutting-edge compliance:** companies that rapidly ensure compliance while innovating will outpace competitors. The deeper a company embeds algorithmic innovation via federation, the more it can capitalize on this advantage.
- **Business continuity:** establishing resilience as a key differentiator allows a company to stand out among its peers, as explored further in chapter 5.

4.3. Core II: E2E On-Platform

With the foundational technology in place from the previous layer, a company can begin building its own end-to-end (E2E) systems for various departments. Think of it as a more ambitious version of today's ERP platforms - broader in scope, deeper in features, and flexible enough to be tailored in the next stage.

This is the layer that shapes the *white collar factory* within a company. Its flexibility often leads to the creation of new, more accurate and efficient protocols, crafted by business experts. These aren't isolated innovations - they're the natural evolution that business professionals across the industry will converge on. Take, for instance, [13],[14],[15], in asset management, a powerful example of industry-wide transformation.

As we'll explore in section 4.5, this layer forms the backbone of the digital brain - the nerve center of a company's advanced transformation. This transformation can move in two directions:

- **Top-down:** Senior management orchestrates the adoption of this layer, designating certain departments or subsidiaries as flagships. These groups pioneer the

[2] Note that not all industries put the same emphasis on both factories. Some industries are balanced towards the blue-collar (such as the car industry), others towards the white-collar (banking and insurance) and others do not want one of the factories (high-end fashion avoids the blue-collar in favor of artisans as part of their brand's signature). It all depends on the nature of the company and its capacity to seek a competitive advantage in one or the other.

changes, inheriting technology, addressing cultural resistance, and establishing best practices that the rest of the organization can follow. Thereon there is a calculated inheritance across departments prioritized by impact in the company's transformation until all the departments that shall be interconnected are interconnected.

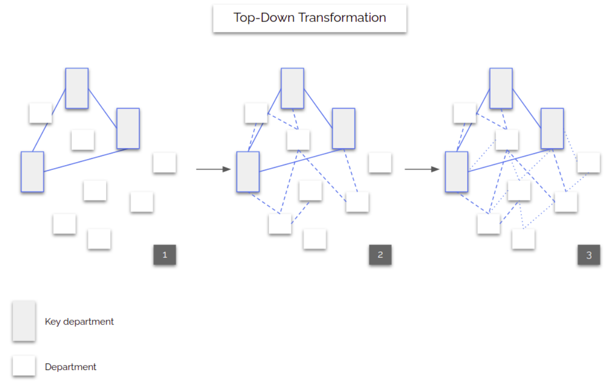


Figure 2. Top-down transformation upon three key departments (or companies within a group) that are first interconnected and then are gradually used to boost the interconnection and transformation of the rest of the departments.

- **Bottom-up:** Crucially, even without a formal transformation project, departments that adopt the Three-Layer Company model in a decentralized manner, independently across departments can still spark a broader company-wide shift. Although this method is less efficient, as the flagships aren't strategically chosen, it leads to the same level of meaningful innovation - only, less efficiently over time.

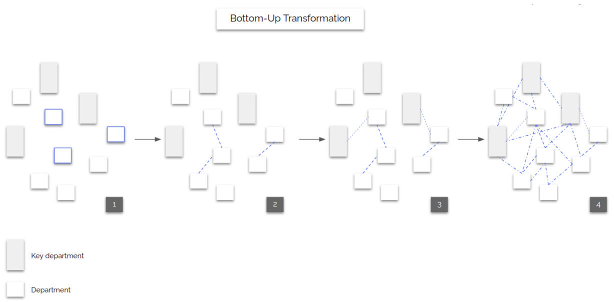


Figure 3. Bottom-up transformation upon the Three-Layer Company model leads to the same point (on-platform organization) yet in a less efficient way as contagion occurs randomly instead of structurally orchestrated.

For a company to truly embrace this transformation, it needs to move swiftly while honoring its legacy. As detailed in [6], the company's existing production architecture must be enveloped in an extended, advanced version. Only then can it maintain pace in a competitive, rapidly evolving landscape.

4.4. Orbit: Idiosyncratic Competitive Advantage

Once teams are equipped with algorithmic-native technology - serving as the foundation for the good-enough version of a diverse range of existing applications of laser-focus nature - they can initiate transformative changes in their operations through:

- **Customization:** They can tailor these technologies in ways that traditional providers, constrained by legacy systems, could never offer. This allows teams to break free from their current technology limitations and push the boundaries of what's possible.
- **Innovation:** Teams can also create entirely new tools that were never available but are essential for boosting efficiency and productivity, moving far beyond their current business model.

Additionally, each department can operate as if they were independent, tech-driven entities - leveraging end-to-end technology that's fully interconnected across the company. This enables every team to customize their tools while still benefiting from shared synergies within the organization.

This process, where differentiation and competitive advantage arise in today's corporate world, also opens the door to new vulnerabilities, which we will explore in chapter 5.

4.5. The Road to ASI

The avid reader may have realized at this point that we believe AI has been given a role for which companies are not ready yet. They miss algorithmic structure before going the extra mile through AI. But that does not mean AI shall be removed from the corporate conversations. It is the North star.

For a company to spend significant amounts of budget on technology it has to be sure that they won't need to change its infrastructure for many years. The abuse of *low-hanging-fruits* in the creation of a holistic platform has led to inefficiencies that ought to be revisited over time. Using patches is a frequent practice that leads to dead ends where, at uncontrolled timeframes, the company needs to set aside major budgets to unlock evolution again or

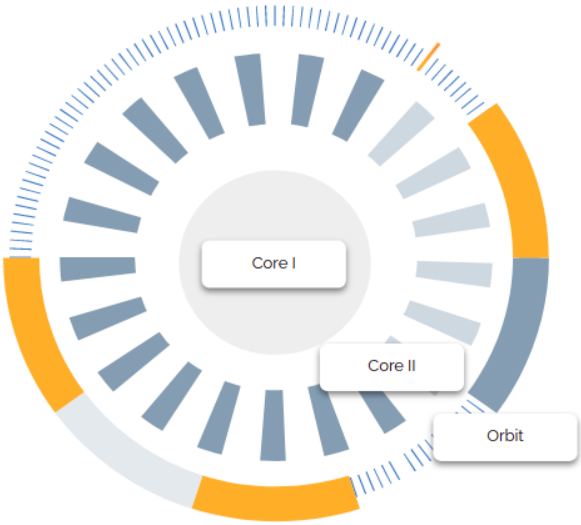


Figure 4. Graphical representation of a Three-Layer Company from [8]

even business continuity - not to settle major competitive advantages.

Paper [5] reviews the far end of a corporate technology, decades ahead, and proposes a technology continuum that can align long-run with short-run targets. It leverages the white collar factories as a common equilibrium across companies that want to succeed via efficiency and productivity. By then mapping those algorithms - which, again, surpass the partial, often outdated views from mere data - with cortex areas in a brain and these, in turn, with Artificial Narrow Intelligences (ANIs), it eloquently defines the ultimate target of a company as the creation of a digital brain that encloses all the know-how of the company, first - Artificial General Intelligences (AGIs) - and thereon, by combining ANIs from the best possible places, their own Corporate Artificial Super Intelligences (CASIs).

Interestingly, those CASIs do not miss the idiosyncratic value of the experts the company accounts for. It is relevant to recall that the aforementioned know-how includes them in two forms:

1. **Rationales:** professionals are the bottomline of the algorithm upon which AI is used as a reinforcer and/or optimizer of the expert's heuristic. Rationales rule the on-platform protocols of the departments and their evolution's impact typically follows a Sigmoid shape for the human, meaning that at the beginning they add key value and as time goes by it becomes more structurally marginal. However, they are still - and will remain so for many years to come - better than machines at detecting changes of data distribution (news, different marketing, new nature of a product. . .) and its consequences. Hence, they can be further incorporated into the CASI through Augmented Machines.

2. **Augmented Machines:** inputs where the human can add value to the machine in ways that haven't been discovered yet - e.g. high frequency research to help a machine decide whether to enter or not into an investment and with which weight (opportunity vs confidence) as in *wallstreetland.xyz*.

Thus, companies have to make sure not only the most power from machines is exploited but also, crucially for decades to come, the role of humans in a corporate world driven by machines.

4.6. Conclusion

In conclusion, the Algorithmization of businesses brings immense opportunities for efficiency and productivity, but it also introduces a new era of cyber threats that are more sophisticated, scalable, and industrialized than ever before.

To navigate this complex landscape, organizations must rethink their approach to cybersecurity, moving away from generic solutions and towards custom-built strategies that incorporate advanced technologies, game theory, and dynamic defenses.

Notably, the more proactive a company is in developing proprietary defense strategies, the more likely it is that some of these strategies will effectively address current and emerging threats. Today, many companies focus on analyzing past attack data, hoping that those patterns will either stay the same or evolve predictably. However, this approach is fraught with challenges - there are often hundreds of different attack methods that can leave similar digital footprints, making it incredibly difficult to pinpoint the exact strategy used.

Rather than relying solely on past data, companies can take control by making it structurally more complex for attackers to deploy any set of strategies. This proactive approach shifts the focus from reactive defenses to preemptive ones, where the goal is not just to analyze attacks after the fact, but to create an environment that inherently disrupts potential threats before they can unfold. By increasing the complexity and unpredictability of a company's infrastructure, it becomes significantly harder for attackers to gain a foothold.

By doing so, they can not only protect themselves from current and future threats but also turn cybersecurity into a powerful competitive differentiator that drives their business forward in an increasingly digital world.

To the light of the former background we are finally ready to show the reader the last zoom-out with regards to the role of advanced transformation in modern cybersecurity.

5. Business Discontinuity: the New BAU as Hackers become On-Platform Organizations

Companies are not accustomed to the level of competition unleashed by the new era of hacking. In terms of innovation, there is an imbalance between the business side and the cybersecurity side of a corporation. While corporate rivals tend to evolve gradually and in a similar fashion, hacking groups operate differently. In cybersecurity, the stakes are exponentially higher, and the race is relentless. The hacking industry, driven by massive profitability, is advancing rapidly towards state-of-the-art Algorithmization, with cybercriminals often building white-collar factories by default. These groups aren't just adopting cutting-edge technologies but are also establishing fake companies to covertly recruit top talent, often without the recruits realizing their involvement in illegal activities. This leads to increased efficiency and productivity, culminating in more intelligent, large-scale, and industrialized cyberattacks - posing an unprecedented threat to businesses. More eloquently, while corporations split their technology budget in improving their blue-collar and white-collar factories, hacking players are 100% focused on their white-collar factory - a 100% focus on breaking a much lower effort.

In this context, understanding how to manage vector attacks within the Algorithmization framework becomes crucial to navigating this new competitive landscape. Leveraging the background gained on the previous chapters, this one covers a series of eloquent examples towards such navigation.

5.1. Federation: the Native First Line of Defense

One of the most overlooked risks in the era of Digitalization is the theft of competitive advantage, particularly in corporate areas with high employee turnover, as noted in 4.2. In the extreme, the intellectual property (IP) of algorithmic-driven departments is just one *copy-paste* away from falling into the hands of a competitor.

Algorithm Protection. Traditional technologies weren't designed to inherently safeguard against this kind of IP theft, often requiring forced, ad-hoc protocols to protect sensitive information. But this is where the logic behind Data MAPs, built upon federated technology[3], comes into play. By breaking software's microservices into even smaller units and distributing them across various apps, algorithms are fragmented into pieces that reside in different nodes across servers. This way, multiple teams can contribute to the iterative evolution of a massive algorithm without any one team having a complete view of the entire system while being natively orchestrated. Federated protocols make IP theft exponentially harder.

Data Protection. When it comes to data, incomplete Federation protocols present a major issue. Arguably, in the context of Digitalization, Federation has not been ambitious enough - merely spreading data across departmental servers for quality and availability falls short of comprehensive protection. Instead, department data needs to be distributed across multiple servers in such a way that, if a breach occurs, only random, unrelated data collections are compromised. For example, a breach might expose a customer's name, an office address, HR feedback for an employee, and the cost of a marketing campaign, but not enough to cause probable damage[4]. An algorithm-driven data management strategy would ensure data availability, while the continual reshuffling of data collections across nodes would add noise to any compromised server. More on this in 5.3.

As will be examined in greater detail, the implementation of Algorithmization at Core I, offers a robust defense mechanism through the federation of algorithms across multiple nodes. This structure not only protects against hacking and external exploitation but also mitigates operational risks. Whether through the inherent advantages of the federated model, as outlined in this discussion, or by leveraging this framework to create new, adaptive security technologies, companies are now able to safeguard their operations in ways that traditional systems are incapable of providing.

[3] Where Federation deals with the optimization between Centralization and Decentralization by seeking the freedom of the latter while exploiting the synergies of the former.

[4] The attacker would require staying in the server long enough to witness significant complementary data. And, in order to extract its value, a high number of iterations across laser-focused algorithms shall be conducted. Thus, a major overall effort. Still, even if successful, only a partial reconstruction of the database that would otherwise be directly available for the hacker.

5.2. Tactical Technology: the CISO's BFF

Once the Three-Layer Company model is implemented, the Chief Technology Officer (CTO) can easily develop ad-hoc tools that enable the business to both thrive and ensure compliance. This model enhances the company's resilience, making it robust against operational risks and hacking attacks, while also supporting business growth and regulatory adherence.

We refer to *tactical technology* as a *good enough* software solution that secures the essential functions of the business. The first step is to identify the company's most critical assets, those that are vital to its ongoing operations and sustainability. These assets must then be replicated internally to ensure absolute control over them, encompassing where they are deployed, how they are protected and how they can be evolved. The first objective from tactical technology is to achieve a robust, basic baseline that can take over the role of a third party software in the face of attacks or operational risk. For that, the company shall leverage technology's algorithmic strategies, as explained in chapter 4.

In this section, we will see the relevance of creating and gradually nurturing tactical technology towards a strategic evolution of its proprietary platform.

5.2.1. The Good Enough of Everything: from Operational Risk Control to Legacy Reinforcement

As a company builds its technology stack, it inherently imports legacy systems from its vendors, often in the form of rigidities. These constraints arise because vendors must design solutions that scale across multiple clients. To overcome these limitations, companies typically engage technology consultants, who serve as the *glue* between disparate software applications. However, this intermediary layer often becomes its own form of further legacy, as consultants also design solutions with scalability in mind, intending to apply them across their broader client base.

Furthermore, since both technology providers and consultants often operate within oligopolistic markets, the standard practices involved in building a technology stack quickly constrain companies across sectors in terms of their ability to differentiate themselves technologically. As a result, Digitalization, rather than enabling differentiation through customization, subtly drives standardization behind the scenes. This limits the company's ability to stand out from competitors, as reliance on widely adopted solutions reduces the scope for unique technological innovation.

This trend poses significant challenges for both business and cybersecurity:

1. **Business:** it introduces two new survival risks. First, there is the threat of disruptive competition from technology providers, who control the legacy systems and gain deep insights into their clients' operations. Second, companies from different sectors that share similar technological legacies may seek to diversify, intensifying cross-industry competition.

2. **Cybersecurity:** standardization exacerbates vulnerabilities. As technology becomes more uniform, so do the nature of cyberattacks. Hackers can focus their efforts on widespread attacks, leveraging the standardized platforms, making it easier to exploit common weaknesses across a broad range of companies.

The solution revolves around the Three-Layer Company model. By leveraging the capacity to create algorithmic strategies the company can disruptively compete with its providers in terms of quality and deployment speed. Note that the target at this point is not to substitute the tech services from those providers but to take over the most relevant pieces of the technology stack, those key to the company, so that it recovers control on risks and evolution[5].

This approach offers significant advantages from both a business and cybersecurity perspective:

1. **Business:** most laser-focused software reaches, say 100% of the standard needs of a company's department on a specific task. And, say, a reasonable effort of three to four months can create, low cost, a good-enough version[6] of all possible laser-focused apps the department needs. But not limited only to those of the department itself but including others from other departments - we refer here to HR to incentivize its members, cyber security to protect their own IP, project management to track how the team works, C-suite level views to understand the evolution of the department's tech... The transformation to white-collar factories and the richness of available technology possibilities means departments' heads are becoming closer to the role of a CEO than of a Managing Director. On top, having

[5] Based on our experience, developing a tactical version of industry-standard software typically takes between 5 weeks and 5 months. The integration with legacy systems generally depends on third-party providers but is usually accomplished within 1 to 2 weeks, facilitated by the increasing API-fication of the technology stack. Once integrated, the continued evolution of the software leads it to become itself the state-of-the-art.

[6] One that focuses on the main usages and leaves outside the tails covered by the industry-standard software.

the ability to interconnect all that technology natively opens up a myriad of possibilities to move from below 100% with respect to the industry-standard benchmark to well above.

2. **Cybersecurity:** the Chief Information Security Officer (CISO) plays a key role in addressing a broad range of operational risks. For instance, a bank can remain compliant with anti-money laundering (AML) regulations even if its third-party provider's servers - those that are currently deciding whether a payment is clean or not - experience a blackout[7]. More broadly, companies could avoid business interruptions due to operational risks like the Crowdstrike outage in the summer of 2024. Had companies deployed tactical technologies on nodes running different operating systems (e.g. Ubuntu), companies would have ensured their core assets continued to operate smoothly despite the external disruption. Thus, this flexibility in cybersecurity architecture enhances resilience and operational continuity in the face of third-party failures.

5.2.2. The State-of-the-Art of Everything: Where Business and Compliance Needs Meet Cyberecurity Needs

Once the tactical technology is in place, covering a wide range of essential services across departments and following the Three-Layer Company approach, the natural progression is continuous evolution. At this stage, the initial implementation is primarily a risk mitigation measure, replicating the company's key assets and applications. But as the organization advances, it begins to allocate efforts around this technology - first, to serve as an additional layer of intelligence, reinforcing existing systems, and eventually, to fully shift roles.

The company's proprietary technology, initially a secondary layer, begins to take center stage as the main application, while the third-party provider's original system transitions into a supporting role, acting as the risk mitigator and reinforcer. This shift is not just about adding complexity but about gaining more control, flexibility, and resilience in the face of evolving challenges.

The smart layer on top: legacy upgrade

Once the company has two software systems running parallel for the same service - its external provider's platform and its own tactical technology - there is valuable insight to be gained from the discrepancies in their outputs. Since these systems are developed independently, any divergence between their results offers an opportunity for optimization.

When the outputs don't align, it signals a decision point. By analyzing the differences, the company can make choices that are likely to be Pareto-superior - meaning they improve outcomes without compromising others - compared to relying solely on the third-party software's output. This dual-system approach not only enhances decision-making but also allows the organization to evolve beyond the limitations of its original tech stack, creating a more adaptive and resilient framework.

Custom innovation and control: take over your legacy

As development advances, this foundational technology gradually transforms into a more sophisticated reinforcement system. At this stage, intelligent, custom-built solutions are layered on top of industry-standard software, allowing companies to significantly enhance their operations while maintaining dependencies on external vendors. This evolution is depicted in the expansion of its representation in step three of Fig 5. The outcome is far from just a temporary safeguard - it represents a robust enhancement of the company's core capabilities.

Once this reinforcement phase is complete, the tactical solutions shift into strategic assets. With greater control over these critical systems, businesses can diminish their reliance on external providers, increasing both their autonomy and flexibility. In the long run, this approach facilitates the creation of a bespoke, adaptable infrastructure that forms a key element of the company's competitive edge. This infrastructure is not only resilient but also adaptive, evolving in tandem with both the company's growth and the threats it encounters.

5.2.3. The Hybridization Consequence: Budget Allocation's Efficiency & Productivity

The challenge now lies not in the Core I technology itself, which has been thoroughly researched and validated by our center of excellence and consultancy firm (see [5] for a description of the group created towards disruptive innovation), but in the allocation of resources. The decisive factor will be how much budget for the construction of the Three-Layer Company is allocated to CISOs by their organizations compared to the resources that cybercriminals

[7] And this, as mentioned above, also leads to the hybridization of business, cybersecurity and compliance. Even more so, as central banks and supranational organizations have already shown interest for their Algorithmization process, next company failures due to the lack of tactical technology may not be considered within the scope of a major force exception but a technology imprudence. And, thereon, a new breed of cyber security attacks seeking this distrust from regulators and bad press will arguably become a reality.

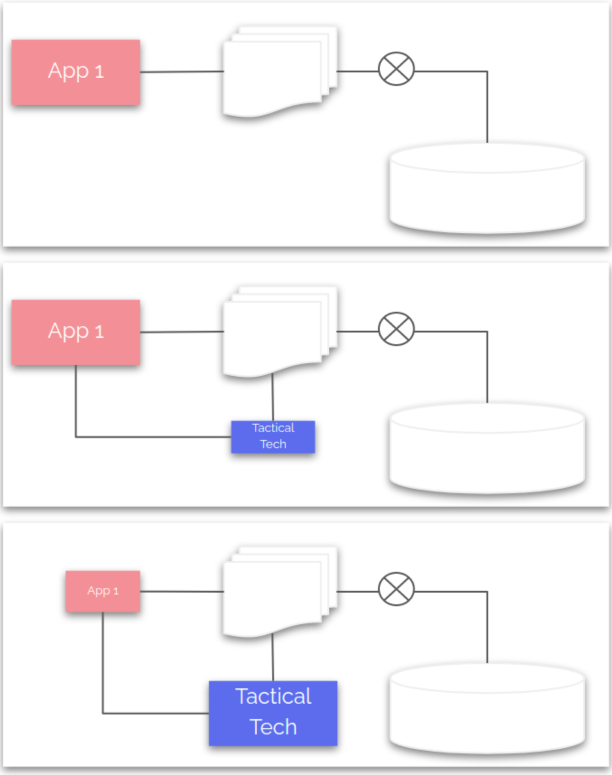


Figure 5. Organic evolution of tactical technology: from reinforcer to leader.

allocate to their *business leaders*. This is, the technology for modern attacks and modern defenses is already here and fully operational; the real battle now is over budget priorities across the two types of *professional* agents.

This budget war is pivotal because it reflects the company's commitment to its long-term security and competitive positioning. A company that understands the importance of this investment will be far better equipped to build the robust, flexible, and internally controlled infrastructure necessary to protect its critical assets. As seen, such an investment on the Three-Layer Company not only safeguards the company's current operations but also positions it for future growth by making it less vulnerable to external threats and business dependencies. Moreover, by unlocking a proactive approach to algorithmic transformation, organizations can shift away from a reactive posture - where they constantly respond to threats as they arise - to start changing the context favorably so that a large number of current risks are naturally neutralized before they become critical.

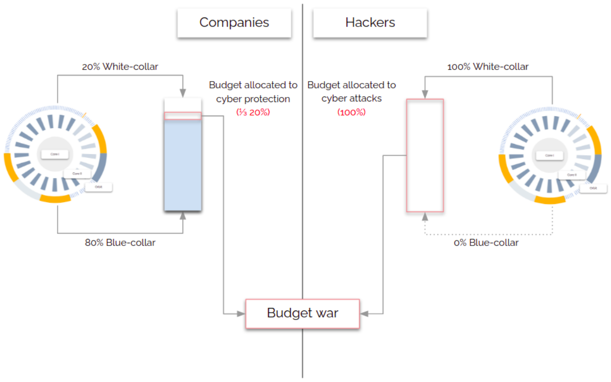


Figure 6. Budget war: eloquent distributions between factories across companies and hacking organizations.

Furthermore, this proactive strategy allows for the seamless integration of new technologies and innovations as they emerge, ensuring that the business remains at the cutting edge without compromising its core systems. As industries continue to evolve and new threats emerge, having a flexible and customizable infrastructure will be a key differentiator, enabling the business to adapt quickly and effectively while maintaining a strong competitive edge. Ultimately, this approach transforms cybersecurity from a defensive necessity into a strategic advantage, one that drives both operational efficiency and long-term business growth. This is where synergy exploitation takes the CISO's budget to entirely new levels. By engaging with Core I, CISOs can bootstrap their resources through several key mechanisms:

1. **Starting from a Privileged Position:** CISOs can reshape the technological context in a proprietary manner by leveraging the distribution of nodes, giving them greater control over security without starting from scratch.

2. **Recycling Resources:** Pieces of technology funded by business or compliance can be repurposed for cybersecurity, maximizing the value of previous investments and reducing the need for additional funding.

3. **Cost-Sharing Opportunities:** Essential components required by both business and compliance can be shared across departments, reducing overall expenses while maintaining robust defenses.

This resourceful bootstrapping allows CISOs to level the playing field, balancing their business-bounded budgets against the attackers' business-driven budgets. While cybercriminals use advanced technology as a revenue engine, corporations often view cybersecurity as a financial burden. However, this approach shifts the dynamic - allowing companies to harness these synergies for long-term security while optimizing financial efficiency.

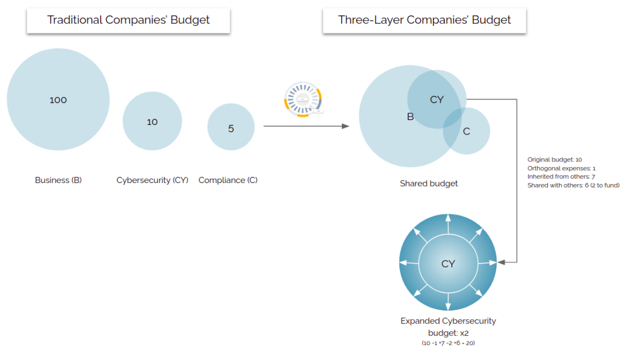


Figure 7. Budget synergies: bootstrapping the Three-Layer Company to double the budget available to the CISO.

5.3. CNE: from the Outlier to the Defaults

Computer Network Exploitations (CNEs) rely on compromising a server and start deep surveillance to gain a thorough understanding of how a company operates. The larger the server and the more centralized its code and data, the easier it becomes for a hacker to grasp significant aspects of the business. By spending time fine-tuning their attack strategy and waiting for the most sensitive time to strike, the hacker maximizes the risk-reward ratio, making their investment in the exploitation highly lucrative.

However, CNEs are relatively rare compared to Computer Network Attacks (CNAs), which are easier to execute and provide faster financial returns. CNAs often aim for quick profits or visibility by causing damage and gaining notoriety.

The question that arises is: Will this trend continue, or should companies expect a shift towards a higher proportion of CNEs in the future? This section aims to analyze the evolving landscape and whether companies need to be prepared for more sophisticated, targeted CNEs in the coming years.

5.3.1. Calm: the New Attribute of Hackers

The parallelization of fine cyberattacks upon algorithmic strategies upon the Three-Layer Company model represents a significant shift in the threat landscape, effectively turning each attack vector into a separate revenue stream for cybercriminals. As these operations become more automated and scalable, hackers will gain the patience and resources (diversification across companies and over time horizons) to focus on highly profitable, long-term objectives.

To defend against increasingly sophisticated cyber threats, organizations must take a proactive and dynamic approach. This strategy includes several key tactics aimed at preemptively neutralizing cyber adversaries and mitigating potential damage:

1. **Agile Simulations:** continuously run simulations that, leveraging Algorithmization, anticipate the evolving tactics of cybercriminals. These simulations should be designed to identify weaknesses before adversaries exploit them and provide valuable insights into potential attack vectors so that a new breed of defenses, based again in Algorithmization, can be designed.

2. **Context changes:** changes the context dynamically in proprietary manners following Game Theory to add noise, confusion and control the extra effort required by the hacking organization to perpetuate a dangerous CNE[8]. E.g. moving parts of the apps (nodes) and data following advanced strategies of hardware and software management. As the attack requires first to solve a massive Game Theory problem, even once inside, the professional hacker will arguably avoid attacking such a company to focus on others with a better level of impact/revenue.

3. **Novel Approaches:** leverage the control of most of the technology to deploy advanced algorithms. E.g. to recycle recent techniques such as Avatar Calibration to monitor user behavior across applications, tracking deviations from a user's typical *avatar* or behavior patterns. This technique helps flag potential user impersonations and enables the algorithmic system to deploy immediate countermeasures, tightening control over fraudulent access attempts.

4. **Automated CERT (Computer Emergency Response Team) Systems:** elevate automated responses to cyber threats by integrating insights from various applications and triggering systematic, algorithmic responses to potential attacks. Similar to algorithmic trading systems in hedge funds (see [13],[14],[15]), these systems should autonomously carry out optimal defense actions without waiting for human intervention. The more tasks that can be automated, the better the response time, with humans becoming the second line of defense.

5. **Augmented Machines and Human Firewall:** while automation is crucial, it's important to maintain human involvement. Experts should be integrated into the loop. It is relevant to the algorithmic-driven defense that humans are given new roles augmenting the

[8] Going forward it is actually a good practice to work with the premise *the hacker is inside* so that risk mitigation mechanisms are steadily deployed in a native manner.

machine or becoming themselves a firewall. Using their expertise to detect anomalies that machines might miss. Humans can provide critical context or even act as barriers to fully autonomous attacks, ensuring that sensitive information, often held only in human minds, remains inaccessible.

By implementing these strategies, companies can create a robust defense system that not only responds to current threats but also anticipates and thwarts future ones, giving them a strategic edge in an ever-evolving cybersecurity landscape.

5.3.2. Game Theory: the Natural Protection to Boost

This shift towards custom solutions necessitates the deep integration of Game Theory into every facet of cybersecurity. Game Theory, which models the strategic interactions between adversaries, provides a framework for anticipating and countering the moves of cyber attackers. By applying Game Theory principles, organizations can design dynamic communication protocols, adaptable architectures, and flexible software systems that not only respond to threats but also actively disrupt the attacker's strategy. For instance:

1. communication protocols could be engineered to change their behavior in real-time, creating an environment of uncertainty that increases the cost and risk for attackers. Similarly,
2. when software architectures are designed following modular components that can be quickly reconfigured, such as those in Core I, the systems can maintain functionality even under active attack. Further,
3. by dynamically moving parts of applications (nodes) and data across different hardware and software, companies can create an unpredictable environment that forces adversaries to solve complex problems before proceeding. This tactic can make targeting the company far less attractive, as the return on investment for a professional hacker decreases in comparison to easier targets.

Moreover, the integration of Game Theory into cybersecurity extends beyond technical measures. It also involves strategic planning at the organizational level, where cybersecurity starts being viewed not just as a defensive measure but as a competitive advantage. Companies that excel in algorithmic compliance and cyber defense will be better positioned to outpace their competitors, not just by protecting their assets but by creating a safer and more trustworthy brand in the eyes of customers and partners. This approach transforms cybersecurity from a reactive, defensive posture into a proactive, strategic asset that can drive business growth, foster innovation, and secure long-term success.

5.4. AI: Ignorance as a Honeypot

On one hand, there's the tool - the innovation of cybersecurity powered by AI. It's crucial to grasp that the current state of data-driven innovation in cybersecurity, given the advanced tactics professional hackers have at their disposal, is prone to significant error. The issue lies in the different nature of the data distribution across observations. As hacking strategies evolve, past data becomes an unreliable guide, representing only a sliver of the potential future threats. Each observation, each attack strategy, is its own beast, and lumping them together is a recipe for blind spots. The true challenge ahead lies in transitioning from data-driven insights to algorithmic simulations - simulations that anticipate not just yesterday's threats but tomorrow's as well. That's where the real evolution in the red and blue team dynamics begins.

On the other hand, there's the usage of AI itself. For cybersecurity officials, this is where the rubber meets the road. They need to rely on machine learning experts who can detect the risks of emerging attacks - attacks that fall in that tricky middle ground between Computer Network Attacks (CNA) and Computer Network Exploitations (CNE). These middle-ground attacks aren't about breaking data but subtly altering it, skewing data - driven models to favor different, unintended outcomes. The standard, straightforward attacks on data are one thing, but the real danger comes from more sophisticated approaches aimed at deeper insights, such as:

- Breaking the underlying assumptions of models, turning them inside out so that their application is wrong by design.
- Exploiting the natural oversensitivity of models - like ordinary least squares (OLS) to outliers, or neural networks to thresholds (issues thoroughly discussed in [5]).
- Exploiting the limitations of large language models (LLMs), which struggle to process outlier information, particularly in summaries. LLMs don't analyze each document on its own terms - they merge it with the memory they've built around related topics, muddying the waters.

And it's not just the data that is at risk. Minor, almost imperceptible variations in model libraries - those little tweaks - can fly under the radar and wreak havoc. This is where real-time control of model libraries becomes essential. Without a strategy to track, audit, and control these libraries as they're being used, cybersecurity teams could find themselves fighting a battle they're not even aware they're losing. Real-time monitoring is no longer a luxury - it's a necessity. The question isn't whether your systems are under attack; it's whether you can see it happening in time to stop it.

5.5. Compliance: Out-of-Business in One Go

As innovation accelerates, so does complexity, and the implications of this evolution are not always straightforward or easy to predict. Governments, in response, are ramping up regulatory efforts, resulting in a web of compliance requirements that often feel like an opaque burden to businesses. Non-compliance can lead to hefty fines and, in some cases, the revocation of licenses, which can dramatically impact both operations and corporate reputation.

Given this intricate and often daunting regulatory landscape, companies tend to allocate minimal resources to compliance, viewing it as a necessary but secondary concern. This underinvestment presents a fertile ground for hackers to exploit.

However, imagine a scenario where the Three-Layer Company framework is fully implemented. In this model, compliance would no longer be a mere regulatory checkbox but a strategic asset. By integrating compliance natively within the company's algorithmic infrastructure, it transforms from a burdensome obligation into a competitive advantage. This approach not only enhances control over compliance processes - through advanced algorithmic solutions - but also allocates resources to safeguard this critical risk vector with the same level of sophistication applied to other areas of the business.

In such a framework, compliance becomes a proactive, integral part of the company's operations, woven into the fabric of its technological and strategic initiatives. This not only mitigates risk but also positions the company to respond more effectively to regulatory changes, turning what is traditionally viewed as a compliance challenge into a strategic asset.

5.6. Market Price Manipulation: Private or Public

Hacking has many more dimensions than most currently recognize, and we are on the verge of seeing these dimensions being exploited in unprecedented ways - particularly in the markets. Rather than simply demanding ransom or causing business disruption, hackers are now eyeing a faster, cleaner profit: leveraging attacks to manipulate markets. These attacks exploit vulnerabilities in a company's business, reputation, and compliance structures and then turn to the markets to reap the rewards.

In a sense, this type of hacking is not too dissimilar from the cutthroat tactics used by hedge funds when they release scathing reports about companies to drive stock prices down[9]. But there's much more beneath the surface.

5.6.1. The Attack: from Our Prediction to a Reality

For years, we've been warning CEOs from companies of all sizes and sectors about the simplest market manipulation strategies that hackers can employ. It wasn't until the highly publicized case of GameStop - where similar tactics were applied but in reverse[10] - that they began to grasp the seriousness of this form of attack.

Here's how it works:

Imagine a professional hacker of this type wants to profit by selling high or buying low. Whether the target is a startup in the private markets (highly sensitive to the aforementioned hacking events), a listed company in the public markets (the smaller the company the more its price sensitivity) or a whole country through the combination of the previous two[11]. An efficient strategy would be as follows:

1. Sells the stock (or buys a put option - the right to sell it at a certain price). It either has notional enough to move the market or convinces a network of other hackers to follow her strategy. As they all sell, the price starts dropping.

2. After selling, they explain why they are selling and everybody should follow them - this part includes fake news and fake social network's agents. It is key to do it as a herd so that the algorithm from the different

[9] E.g. Gotham City Research on Grifols in early 2024.

[10] That actually wanted to take a hedge fund down, not a listed company. As the hedge fund was short of the stock, the strategy was to increase the price of the stock by buying it - adding a romantic component for everyone not to feel a hacker but a savior of the stock instead.

[11] [10], a paper we created for NATO, further reflected on the geostrategy implications of such an approach. A country can take over another one without needing to fire a single shot. Just by hacking the companies value in the markets, controlling the country via boards of the main companies and making profits in the interim.

social media overweights the relevance of their topic and prioritizes it.

3. Real investors see the price drop and start to worry. They search for information, and search engines lead them straight to the hacker-generated content - by design of the search engine algorithm. Thus, given the misinformation, the risk aversion and the behavioral biases, a significant amount of them start selling. The price drops again.

4. Real algorithmic investors keep selling as there is a pattern already in the data of the stock - both in prices and media. The stock falls even further.

Along this path, represented in Fig 8, tens of millions, if not hundreds, are wiped from the wealth of the company's investors. Thus, arguably, investors will demand their assets to be appropriately safeguarded going forward. In particular, the protection service will be business-as-usual on companies with large, concentrated ownership (like family-controlled businesses).

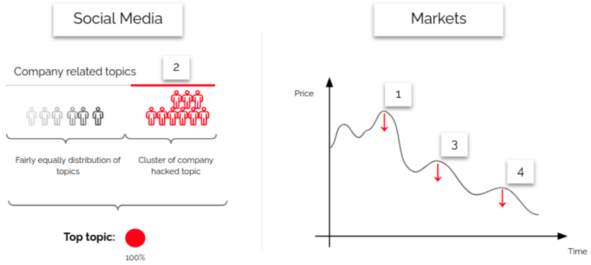

Social Media
Markets
Company related topics
2
Fairly equally distribution of topics
Cluster of company hacked topic
Top topic:
100%
Price
1
3
4
Time

Figure 8. A novel, highly effective hacking strategy to manipulate private and public market prices.

5.6.2. The Defense: the Beauty of All-in-One Platforms

A company that has implemented the Three-Layer Model can orchestrate algorithmically, as represented in Fig 9, the response to these attacks through the Communications department and the CFO's office when particularly when algorithmic trading is available within the Core II layer.

1. The first price drop due to market impact can't be avoided. But it can be noticed by the CFO's algorithmic trading algorithm.

2. The misinformation on social networks can't either be avoided. But it can be noticed by the Communications' brand's tracking algorithm.

3. The Communications team then deploys a counterattack. They flood the same social media platforms with accurate, official information at the same scale as the misinformation, mirroring the number of likes, shares, and comments generated by the hackers. For that they leverage curated, autonomous agents[12].

4. The CFO starts building stock treasury inventory with the aggressiveness and urgency that depends on the signals coming from the Communications department - their brand's tracking algorithm.

5. When investors check the stock price they may notice the effect from (1), but a part of it will be already eroded by (4) and, even if the drop was as much as in the previous case, when they wanted to search for information on the company, the algorithm would have positioned on top both news - the hacking and the official response. Hence, the drop in price due to those that still want to sell would be much lower.

6. Data patterns would be broken already by (4) in a savvy manner so that algorithms would not trigger any further sell and thus, the movement won't be amplified.

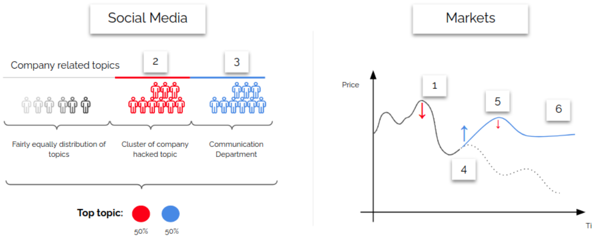


Figure 9. The algorithmic response, across departments, showing the roles and dynamics in countering market manipulation.

Best of all, this strategy is systematic, transparent, and fully auditable. It's not just compliant with regulations - it's effective, turning a hacker's attempt at market manipulation into an opportunity for the company to show its resilience and protect its value.

5.7. Conclusion

A myriad of new risks have emerged, and prioritizing them effectively is now more crucial than ever. One of the most challenging aspects of Transformation is self-criticism. Human nature tends to resist change and favors maintaining momentum, even when that momentum stems from outdated protocols. Many of these protocols, strongly

[12] Note the synchrony between machines tasks and humans tasks in this example.

embedded in company operations, are actually patches - temporary solutions that addressed limitations from years ago, not what was ideal. The disruptions caused by innovations like Data MAPs and the Three-Layer Company model open up new possibilities, enabling the realization of once impossible objectives across every department of a company.

We have discussed several new protocols that emphasize the hybridization of departments - be it tech-focused as in 5.6, or related to budgeting as in 5.2 - while preserving crucial autonomy through a federated structure. This is what defines a modern company.

And with modern companies comes the need for modern cybersecurity. It is no longer simply a matter of keeping up with business evolution; cybersecurity has become essential because hackers are becoming increasingly professional, and they will undoubtedly exploit the advancements made by these modern companies. Consequently, companies must start orchestrating themselves in new, sophisticated ways. The attacks of today - and especially of tomorrow - won't just aim to disrupt; they will be more targeted, seeking to inflict damage across multiple dimensions of a company.

These new risks must be acknowledged, and the old, comfortable risks we've grown used to should be reprioritized in light of this evolving landscape. Transformation is not only about chasing new opportunities, but also about recognizing the new vulnerabilities that come with them - and addressing those with a proactive, strategic mindset.

6. Conclusions and Future Work

Throughout the paper, we have arrived at the conclusion that the same way as modern AI will not be data-driven but algorithmic-driven, as thoroughly explained in [5], modern cybersecurity will follow the same path.

Digitalization is advancing towards Algorithmization so fast that past data is now too vague, too outdated, to offer real insight for today's defenders. It's merely a snapshot, a fragment of the kinds of attacks that could happen. And as the potential for new forms of cyberattacks grows, what truly matters now is stressed data - the simulated scenarios that push systems to their limits, offering a glimpse of the future threats that might emerge.

As a result, developing autonomous and highly advanced cybersecurity strategies is no longer just a best practice; it is an imperative - to move from passive to proactive defense. These strategies must be designed to introduce a level of complexity and unpredictability that significantly raises the bar for attackers. The future of cybersecurity will depend on the deployment of intelligent, large-scale, and industrialized defenses that are capable of matching the sophistication of the threats they are designed to counter. By mirroring the capabilities of cyber adversaries, these defenses will not only protect current systems but also enable organizations to innovate new architectural and protocol flexibilities, enhancing their resilience and adaptability in the face of ever-changing threats.

One of the most critical aspects of this approach is the shift from generic, off-the-shelf cybersecurity solutions to custom-built strategies, tailored to the specific needs and vulnerabilities of each organization, and capable of leveraging Game Theory towards adding noise to the modern hacker. Off-the-shelf solutions, while convenient, are inherently more vulnerable to exploitation because they are standardized and widely understood. Cybercriminals can study these solutions, identify their weaknesses, and develop industrialized attacks that can be deployed across multiple targets. In contrast, custom-designed cybersecurity strategies introduce unique layers of complexity that make it exponentially more difficult for attackers to systematize and scale their efforts. Modern technology platforms are crafted rather than stuck. By incorporating bespoke elements into their defenses, organizations can create a moving target - literally, through algorithmic-driven core technology such as Data MAPs - that is much harder to penetrate.

The work of our Centre of Excellence will be devoted to, in the near future, leverage its pioneer exploration of the Algorithmization process. And being cybersecurity one of the most critical fields impacting society today, it will devote part of its resources to the herein borned greenfield: the arms race between Algorithmic Cybersecurity and Algorithmic Hacking. We shall use our Three-Layer Company platform to produce more research that helps train blue and red cybersecurity teams to navigate this new era appropriately. And we will further investigate use cases that educate companies on how to bootstrap IT budgets by hybridizing business, cybersecurity and compliance when deciding their technology. Such a technology should gradually move from an amalgamated stack of third-party software to an algorithmic-native, proprietary platform - respecting the legacy through an Extended Production Architecture as explained in [6]. Instead of evolving the greenfield independently, the idea is to collaborate with CISO's associations all over the world to grasp intelligence on what is most relevant for them overall, which parts they do not fully understand, etc so that future ad-hoc, proprietary solutions are rapidly unlocked across sectors. This is, more than mere theoretical evolution we target impact. On that note, this initiative will kick off with the ISMS Forum, serving as a starting point for broader engagements with cybersecurity professionals worldwide.

This is more than just a technological leap - it's a fundamental shift in how companies should think about cybersecurity, making it a core, algorithm-driven component of their strategy for the future.

References

[1] Drayer, P., Jones, T., Klima, T., Oberholtzer, J., Srong, A., Welburn, J., & Winkelman, Z. (2018). Estimating the Global Costs of Cyber Risk. Justice, Infrastructure and Environment. Rand Corporation.

[2] Gavenaite-Sirvydiene, J., Miecinskiene, A. (2021). Forecasting Costs of Cyber Attacks Using Estimation The Global Cost of Cyber Risk Calculator V 1.2. Conference: International Scientific Conference ,Contemporary Issues in Business, Management and Economics Engineering.

[3] López Gutiérrez, J., Sánchez Jiménez, F., Herrera Sánchez, D., Martínez Moreno, F., Rubio García, M., Gil Pérez, V., Santiago Orozco, A., Gómez Marín, M. (2020). Informe sobre la Cibercriminalidad en España. Secretaría de Estado de Seguridad (Ministerio de Interior).

[4] Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., Schwarzenbach, A. (2020). National Cyber Power Index. Belfer Center for Science and International Affairs (Harvard Kennedy School).

[5] Alvarez-Teleña, S. and Díez-Fernández, M. (2024). Advances in Artificial Super Intelligence: Calm is All You Need. SSRN.

[6] Alvarez-Teleña, S. and Díez-Fernández, M. (2022). Data MAPs: On-Platform Organisations. SSRN.

[7] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Transformation: Why and How CEOs are Moving from Digitalwashing to White Collar Factories. SSRN.

[8] Alvarez-Teleña, S. and Díez-Fernández, M. (2024). The Lean Aggregation Behind the Next M&A, Tenders and Organic Growth: Federation and the Three-Layer Companies. SSRN.

[9] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in AI: When Applied Science is not Science Applied. SSRN.

[10] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Cognitive Warfare: Augmented Machines upon Data MAPs towards a Fast and Accurate Turnaround. SSRN.

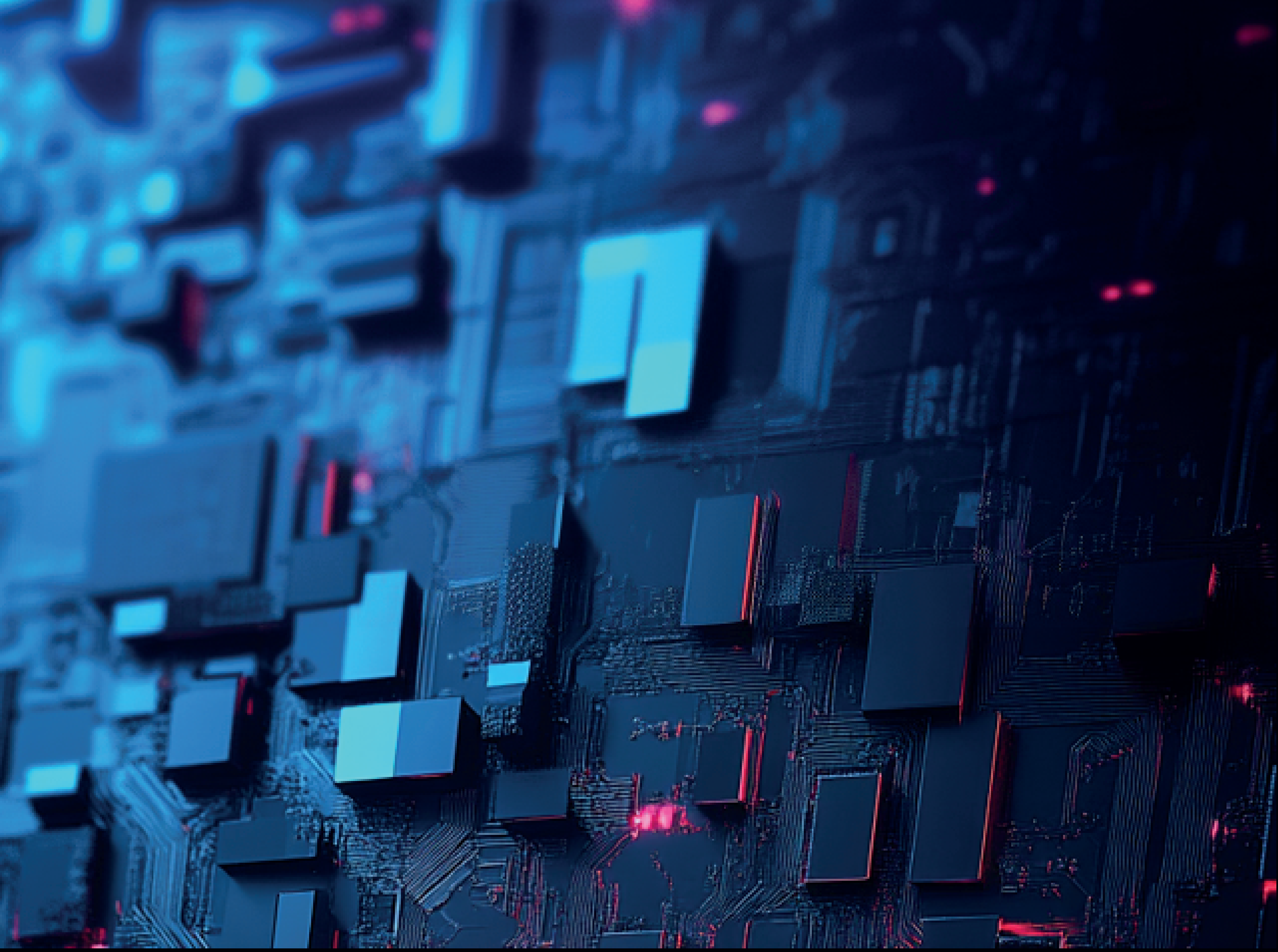
[11] Alvarez-Teleña, S. (2024). Transformación Avanzada. 3648, La Inteligencia Artificial Aplicada a la Ingeniería Civil. Revista de Obras Públicas.

[12] Alvarez-Teleña, S. and Díez-Fernández, M. (2024). Transformación Avanzada. Recuperando el Liderazgo Militar en Innovación. 80, Boletín de Observación Tecnológica en Defensa.

[13] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Portfolio Management: Dimension-Driven Portfolios. SSRN.

[14] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Portfolio Management: On-Platform Performance Attribution. SSRN.

[15] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Portfolio Management: On-Platform Governance for Portfolio Managers. SSRN.



CONTACT US

If you are interested in collaborating with us or need more information about our projects, please write to us at:
proyectos@ismsforum.es