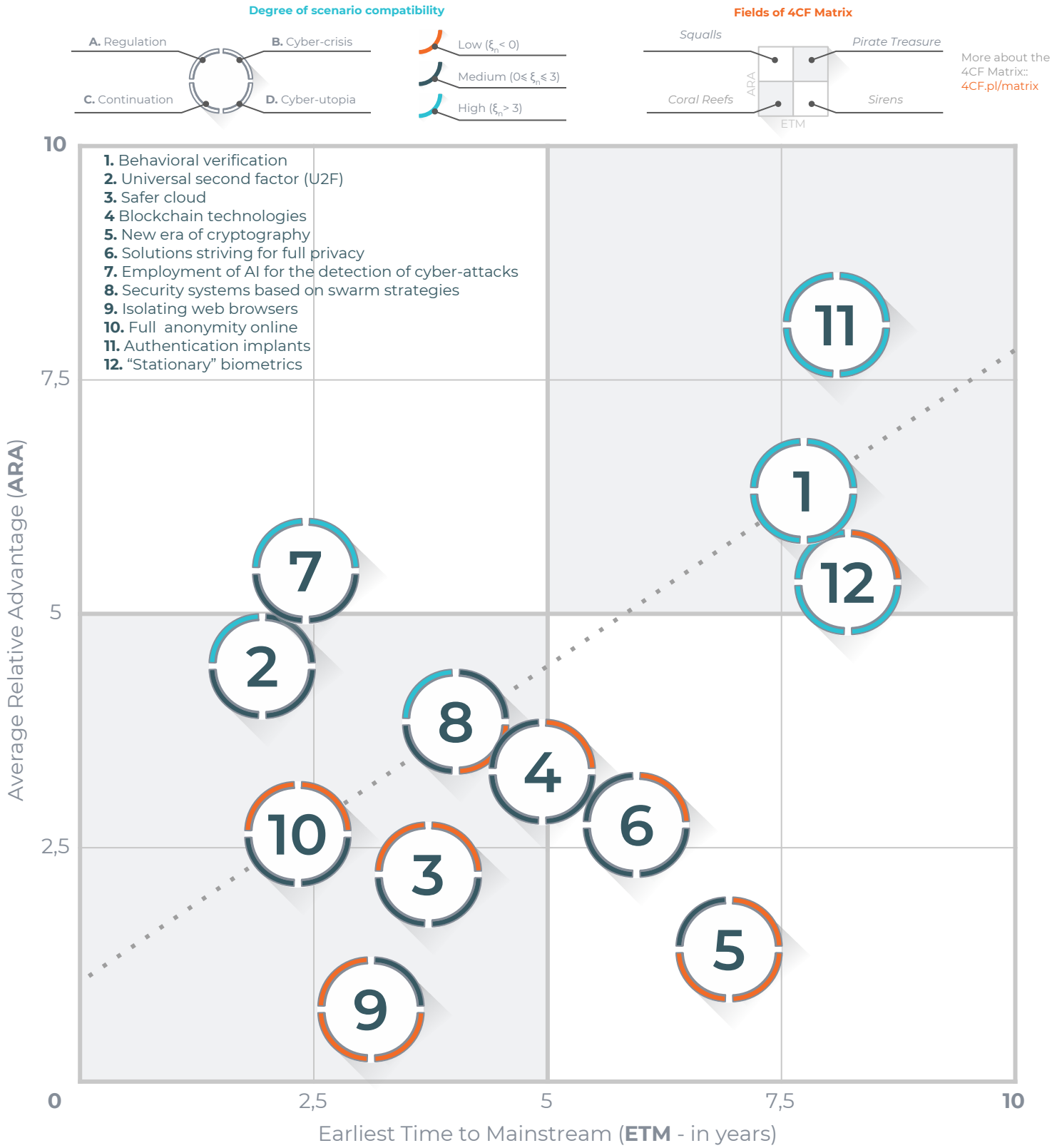

EUROPEAN
CYBER
SECURITY
MONTH
4CF
Surf the future
the unexpected future:
CYBERSECURITY
4CF MATRIX
2018+10

# 4CF MATRIX: **CYBERSEC 2018+10**

The future of cybersecurity is not set in stone: it is being shaped by a number of factors. How to gain a strategic advantage and surprise your market competitors without getting surprised yourself? The 4CF Matrix is a tool for long-term strategic analyses and has successfully been applied in a broad range of fields (including FMCG, the medical industry, banking or military applications). It is typically used to analyse a specific organisation with regard to its strategic goals, market segments and needs. It helps to establish a development plan based on insights into the future which are unavailable to one's market competitors. The following version is public and general, but contains valuable information. We invite you use it as a point of departure for an in-depth analysis from the perspective of your own business.

The 4CF Matrix is defined by two axes: **ARA** - *Average Relative Advantage* and **ETM** - *Earliest Time to Mainstream*. ARA is a complex measure, averaged for future scenarios. It takes into consideration the pros and cons of a specific solution as opposed to alternative options with regard to future needs. ETM is expressed in years (counted form 2018) and signifies the earliest possible time of dissemination. ETM is not a prognosis, but it might be too late to respond to market changes after the deadline that it defines.



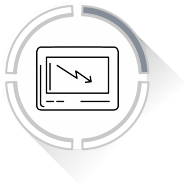
# SCENARIOS: CYBERSEC 2028

When thinking about the future we have a tendency to extrapolate current trends and to assume they will remain unchanged in the coming years. The future, however, is not predetermined and it may follow various paths. In the coming decade, cybersecurity will be influenced by a number of factors, the most important of which have been analysed and grouped into four clusters, thus defining four future scenarios. One of them is a continuation scenario which corresponds to a simple extrapolation of current trends. The other three describe variants of the future, in which one or more of the current trends will change, thus significantly modifying the rules of the game. Confronting specific solutions with the possible scenarios allows you to determine whether the solutions are resistant to changes in an ambient environment as well as to establish the conditions which would best serve a particular solution.

## A. REGULATION

Pleased with the effects of regulations introduced in 2018 (including GDPR in the EU, and ACTA2) many governments and international organisations decided to further regulate cyberspace. The 3rd decade of the 21st century saw the introduction of new laws, intended to muzzle online activities. A number of new solutions were gradually introduced over the years: a legal requirement for hardware to be safe and immune to cyber-attacks (the „secure by design" philosophy"), a requirement for companies to increase spending on cybersecurity, the creation of state and international agencies responsible for security on the web. The market's development slows down and online services become more expensive. In 2028, despite protests, a radical new law results in the beginning of the so called Internet 2.0. Each user is identifiable and detectable, bots and AI have assigned owners who are responsible for their actions.

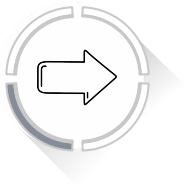
It seems that the wild wild west era of the web has come to an end, but not all consumers are pleased. Some enjoy the security provided by the restrictive regulations, but many - discouraged by the constant surveillance and the increased prices for network services - are looking for privacy in alternatives to Internet 2.0 which are not entirely legal.



## B. CYBER-CRISIS

Decades of hard work in the 2020s resulted in proving the Riemann hypothesis, the key to the discovery of prime numbers that form the basis of current cryptography. Along with the increasing computing power available to cybercriminals and the still imperfect software, it means the world is facing the threat of chaos, associated with the inability to combine the convenience of data access with security. A global race has begun to create new, effective encryption and authentication methods. Unfortunately, it is too late. In 2028 a series of huge cyber attacks occurs, and the level of online security is decreasing dramatically. Financial institutions are suddenly forced to go offline. An economic crisis begins, financial institutions and technology giants are paralysed, governments are accusing each other of supporting cyber criminals. The world is facing the threat of a Third World War.

Consumers are terrified of losing data and financial resources. They are ready to give up convenience in favour of increased security, which in many cases results (at least partially) in a return to offline solutions.



## C. CONTINUATION

The IT industry is developing. IT giants as well success-hungry startups have flooded the market with IoT equipment. As a result, in 2028, humanity entered a full-fledged "smart era". Most everyday devices are equipped with modules for collecting and sharing data, which, analysed by advanced artificial intelligence algorithms, becomes the foundations of new products. This technological prosperity, however, has its price: along with the increase in the number of IoT devices, the number of cyberattacks is also growing. These include onerous DDoS attacks. Not only criminal groups pose an increasing threat, digital armed forces are an indispensable element of armies, the first open conflicts in cyberspace erupt. The Internet is no longer a casual place. Internet users are more cautious and IT companies prioritise security. Various forces are kept in a state of shaky balance, cyberspace is creaking from the tension and a global conflict seems a matter of time.

Consumers are stuck between concerns about data security, privacy and convenience. Most use the widely available online services and believe that they are relatively secure. Regular reports about huge hacker attacks, however, bring awareness to consumers regarding issues related to cybersecurity.

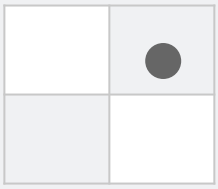
## D. CYBER-UTOPIA

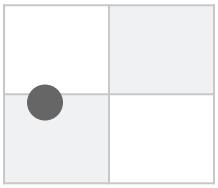
Due to a visible slowdown in the growth of computing power, the scientific and business communities associated with the IT industry started searching for new solutions. In 2028 there is a breakthrough: IT solutions based on photonic and quantum technologies become reliable and affordable for businesses, so they quickly gain users. It will take at least several years before it is possible to produce a quantum smartphone, but the incredible increase in computing power, combined with a new, quantum approach to encryption, cause the security of sensitive digital data to increase rapidly. The owners of quantum solutions limit their accessibility to specific applications, i.e. research and safety mechanisms in finance. Private users are not granted access, so as to avoid arming cybercriminals. It seems that, at least for a few years, the threat of a cybersecurity crisis will be kept at bay.

Consumers quickly become very accustomed to this new, wonderful world. They are more willing than ever to entrust their data to external entities and widely use increasingly advanced network services, including AI virtual assistants, who can access even the most intimate information about users.


### 1. Behavioral verification

User identification based on reflexes or behaviour (the fact that these are difficult to control increases security). For example, the user types a text fragment and the system compares his/her way of writing with the expected pattern. Future possibilities are even more interesting: the study of reflexes, the pupil's response to a flash of light, or blood pressure spikes caused by visual content. In the long run, this method has received a very high rating.





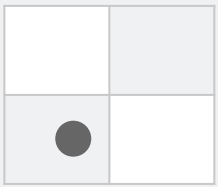
### 2. Universal second factor (U2F)

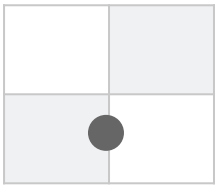
User identification by means of additional equipment intended solely for this purpose. Such solutions are developed by the FIDO Alliance (Fast IDentity Online) consortium, and include, for example, the YubiKey developed by Yubico. In order to avoid the problem of unauthorised usage (e.g. as a result of losing the key), additional security measures should be employed, such as a PIN or biometrics.



### 3. SAFER CLOUD

Users have the option of entrusting their data to specialised companies through a cloud-based service. The data may be protected, for example, with the employment of lattice cryptography - a solution that masks data converted in clouds provided by third parties.





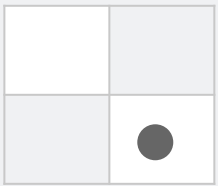
### 4. Blockchain technologies

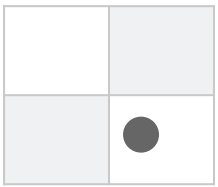
Maintaining anonymity and data uniqueness by using blockchain (a data verification system which uses past data from the transaction chain) could prevent sub-supplier fraud (at the supply chain level) and facilitate the fight against fake news. Compared to alternatives, the method obtained a moderate ARA rating.



### 5. New era of cryptography

The next generation of data encryption algorithms, e.g. the next version of the SHA (SHA-4) standard. Using the ever-increasing computational power of devices available to average users, cybersecurity specialists are developing more complex encryption algorithms which are harder to crack. Encryption based on the DNA code may be a breakthrough in this field. Despite these hopes, this is only a treatment of symptoms, rather than a solution at the root of the problem. It is unlikely to permanently change the face of cybersecurity.





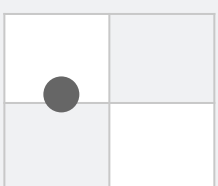
### 6. Solutions striving for full privacy

Solutions which provide the user with full control over their online data (e.g. the SOLID platform - social linked data) and thus reduce vulnerability to attacks. The user's data would be placed in specific locations on the web, known to the user. Any service wishing to use such data would need consent. The solution might improve privacy, but would not impact other cybersecurity issues.



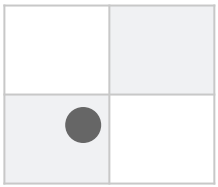
### 7. Employment of AI for the detection of cyber-attacks

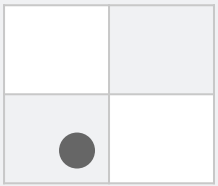
In the case of DDoS attacks, the primary defence is early detection. Tools based on artificial intelligence (deep learning, machine learning, neural networks) might become a substantial aid. They could be used to help recognise patterns of behaviour characteristic of malware attacks at a very early stage and to nip them in the bud. This solution is a potential game-changer.




### 8. Security systems based on swarm strategies

Advanced social structures created by animals and the strategies they employ may be a source of inspiration when it comes to potentially effective solutions for the detection of cyber attacks. A good example is the HONED algorithm (Hive Oversight for Network Intrusion Early Warning using DIAMoND), which employs an effective strategy to provide alerts about system anomalies, and which is inspired by the behaviour of bees.





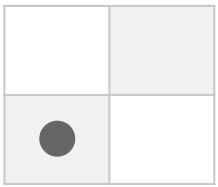
### 9. Isolating web browsers

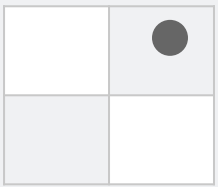
Physical isolation of web browsers/internet connections from data infrastructure and internal networks (of organisations). It reduces the risk of internet attacks on the system almost to zero. A slightly less secure, but more convenient solution, is the service of remote isolation. A company may purchase access to servers on which it will use browsers. If an infection occurs, it is the service provider's machines that are exposed.



### 10. Full anonymity online

The possibility to conceal your identity online while maintaining authorisation capabilities could greatly increase the safety of Internet users. One of the tools which may contribute to such a development is the zk-SNARK algorithm. It is based on *zero-knowledge proof* and the anonymisation/pseudonymisation of data. But will complete anonymity not encourage cybercriminals to act more aggressively? This risk significantly affects the assessment of the solution.





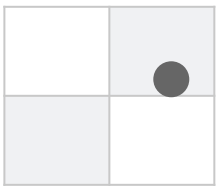
### 11. Authentication implants

In the simplest version, it is an implant which allows the user to authenticate and authorise payments in a manner similar to contactless payments. In a more advanced version, it additionally verifies the identity of the "carrier", and activates only on cue, e.g. after a specific hand gesture which serves as a declaration of will. It is a definite leader in the current study, but still needs a lot of time and further development before it can enter the market.



### 12. “Stationary” biometrics

Despite the entry of biometrics into the mainstream (fingerprinting in smartphones, face scans), we are still unable to pay for purchases with "ourselves" - without a wallet, phone or other accessories. Stationary biometrics may be the answer, but it would need to provide users with a sufficient level of security ("My iris scan/capillary grid pattern cannot be stored in the terminal where I paid"). It would also have to increase the convenience of use (biometrics happening "in the background").



---

SHA - *Secure Hash Algorithms* - a family of rules (cryptographic functions) that convert user-entered content (e.g. password, login, credit card number) into a 40 digit number in hexadecimal code. The third iteration of this family, SHA-3, is currently the main standard for encrypting data on the Internet.

Zero-knowledge proof - a communication protocol that would allow one side of the dialogue (Interlocutor A) to prove to the other party (Interlocutor B) that he possesses knowledge about the value of X, without revealing any additional information beyond this single fact of possessing knowledge. Interlocutor A does not disclose the value of X to Interlocutor B, he only informs B that he knows what the value is. This greatly contributes to the strength of this protocol.

Anonymisation - a method of ensuring privacy by removing all information that could identify the user form the data that he entered.

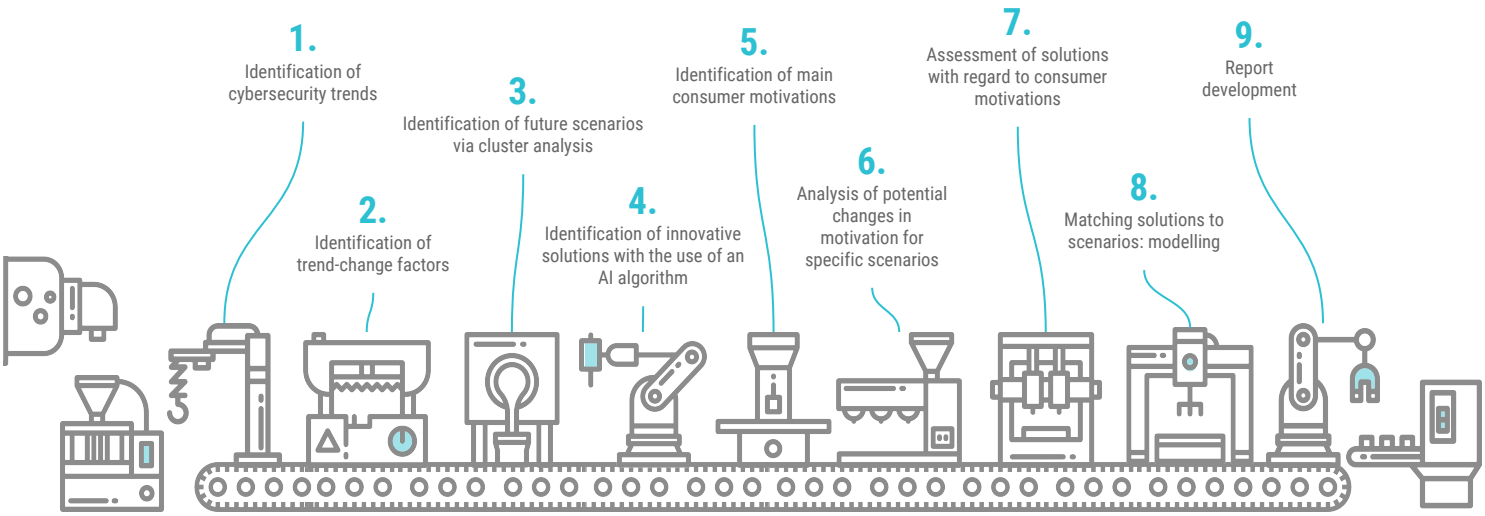
Pseudonymistaion - a method similar to anonymisation, the difference being that the data, rather than being removed, is concealed under a pseudonym.

DDoS - *Distributed Denial of Service* - a type of cyber-attack which "clogs" the server containing, e.g., a website with millions of requests for access generated by devices controlled by the cybercriminal (bots, zombie-bots). The effect is a temporary lack of access to a given service.

IoT - *Internet of Things*. A term that describes the phenomenon of "connecting" various items of everyday use, whose primary function is not related to communication (toothbrushes, refrigerators, various markers to collect and send information), to the Internet. These objects collect data and send it for further analysis. They also communicate with each other (e.g. a keychain "talking" to the door lock). In 2017, almost 9 billion such devices were connected to the network. It is estimated that in 2020, their number will exceed 20 billion.

# THE REPORT: MAKING OF

This report is the result of a complex, methodologically advanced analytical process which aims to ensure the highest possible level of quality and to provide an adequate scale for the assessment of potential future solutions.
The 4CF team would particularly like to thank Karol Chwastowski, Grzegorz Małecki, Marcin Strzelecki, Tomasz Jędrkiewicz and Aleksandra Świączkowska for their assistance and consultations, which were indispensable in the preparation of this report. The report was created in cooperation with the Polish Society for Future Studies, as part of the European Cyber Security Month.




# WHAT'S NEXT?

Were you surprised by any parts of the report? Do you disagree with any of its aspects? What is your opinion of the scenarios: which bring promise and which might prove dangerous? Are there some solutions you would rather see fail or some that you might try to win the market with?

Rapid market changes make it harder to develop a future-safe strategy. The conclusions this report proposes will help you identify areas of particular interest for your organisation. However, to surprise your competitors on markets of the future and avoid being surprised by market developments, you might need a more in-depth analysis, which would consider a wider range of solutions, your strategic goals, market segments, your capabilities and needs. Such an analysis, along with the constant monitoring of the environment in search of early warning signs, is the key to *surfing the future*, in other words: shaping desired future scenarios and using the changes to achieve your long-term development goals. You should remember that many organisations, including your competitors, already utilise analyses similar to this one. Those analyses, however, are confidential, considerably more elaborate and are being used with a future strategic advantage in mind.

4CF Surf the future

4CF is a strategic foresight consultancy with global reach. We have been helping our clients reach the best strategic decisions for over a decade by making sure they stay a step ahead of competition. We help our clients to safely surf the wave of change but also to use market changes to their own advantage more successfully than their competitors.

Providing insights into the future which help you reach strategic decisions is a task we take very seriously. Our advanced research methodology, which places us in the global forefront of business foresight, is constantly being enhanced. That is why not only corporate clients (Asseco, First Data, Skanska, BGŻ BNP Paribas, Deloitte or Kongsberg) but also international organisations and government institutions have trusted our services.

www.4CF.pl
info@4cf.pl
(+48) 22 24 72 772
fb.com/4CFuture