DANUBE
INSTITUTE

Chinese AI Capabilities in Hungary: An Assessment

Logan West

Matthew McCracken

Eric Hendriks

Wael Taji

Jan 2024

Chinese AI Investment in Hungary: An Assessment

Logan West, Matthew McCracken, Eric Hendriks, and Wael Taji

Abstract

The realization of artificial intelligence research and development in Hungary by Chinese entities has raised concerns about potential intentions and capabilities that could materialize in the future. An issue that results from acting on such concerns is that they originate from a position of theoretical danger rather than a substantiated history of hostile actions due to AI's advent being so recent. The ongoing development of both the capabilities of AI and an understanding of those capabilities as well as the opaque nature of Chinese politics provide additional layers of ambiguity which highly complicate efforts to determine what dangers exist and their likelihood for occurring. In the context of Hungary, such questions are pertinent due to the development of AI-augmented state-level infrastructure and large commercial assets. In addition, Hungary's international security and economic relations are also concerned due to perceptions that Hungary is not positioned to address such issues. The objective of this report is to detail what assets exist in Hungary that make use of artificial intelligence, what malicious capabilities artificial intelligence may have that apply to such assets, and under what circumstances Chinese actors would pursue their utilization. Finally, general recommendations are proposed with a goal to ensure Hungary's security relations with other nations remain assured, whilst not unduly damaging its commercial relations with China.

Keywords: *Hungary, Chinese FDI, capabilities, IFF, Artificial Intelligence*

Introduction[1]

The Central European nation of Hungary has recently become a point of focus in the growing realm of cyber geopolitics - a development that is largely due to the technology-focused relationship between Hungary and the People's Republic of China. The backbone of this relationship has taken the form of investments made into Hungary's telecommunications infrastructure as well as various artificial intelligence research endeavors. The results of these efforts include Hungary's 5G telecommunications network constructed by the China-based technology company Huawei, the East-West Intermodal Terminal which is the world's first freight terminal augmented by artificial intelligence, and research and development centers such as the European Supply Center to study the capabilities of artificial intelligence in state-level infrastructure. The Budapest-Beijing relationship is one that has positioned Hungary as a center of gravity for state-level cyber capabilities in the region. However, this relationship and its results have produced issues that have brought Hungary into contentions with its security allies in the West.

A concern has begun to formulate in the minds of Western defense and security analysts with regards to cybersecurity when considering the proliferation of Chinese telecommunications technology throughout Europe, with Hungary being an early adopter.[2] Considering that Hungary is a member of the NATO alliance and a member state of the European Union, there have been questions emerging on what vulnerabilities Budapest's relationship with Beijing may entail. Concerns range from infrastructure being shut down to being manipulated for malevolent purposes at both the state level as well as throughout the region in which Hungary could potentially be used as a "beachhead" for wider ambitions directed towards the rest of Europe. While concerns are understandable given the current tensions between China and Western nations, the conversation concerning what risks Chinese built-infrastructure poses has primarily been theoretical while not taking into account what actual intent and capability exist.

The purpose of this report will be to offer an analysis of what potential vulnerabilities may exist to Hungarian infrastructure and international relations based on the capabilities and intent of Chinese cyber-augmented assets and infrastructure. With regards to capabilities, most of the analysis presented will be hypothetical due to the nebulous nature of what actual control China may have over Hungarian infrastructure, both from a technical standpoint. The resulting analysis is intended to provide an overview of what conditions China may consider exercising manipulation over Hungary's cyber-augmented infrastructure and what form it may take.

Historical Background

Since the fall of the Berlin Wall, Hungary and China have made efforts to develop economic relations with special attention being paid to its economic sector. Since 2019, these endeavors have focused on the realm of cyber-augmented infrastructure and artificial intelligence (AI) research. Hungary has become the center of China's telecommunications efforts thanks to its balance of relations between the East and the West. While maintaining its position as a member of both the European Union and the NATO alliance, Budapest has also made efforts to maintain its connections to eastern powers through endeavors such as the Eastern Opening Policy that promotes investments from East Asian nations such as China, Japan, Taiwan, and South Korea. China's courting has had a dual motivation for both economic development as well as "geopolitical considerations" such as China's peace plan proposal for the war in Ukraine.[3] Results have primarily materialized in the realm of automotive-related manufacturing, but in the case of its business with the People's Republic, most benefit has come in the form of technological development, primarily in telecommunications, logistics, and manufacturing.

In the case of China, much of this investment has come with a common underlying focus of 5G networks and AI utilization in state-level infrastructure. Logistical assets such as the East West Intermodal Gateway have served to promote Hungary as a node for European freight by implementing the world's first artificial intelligence-augmented railyard to optimize cargo handling. Other projects include the construction of the nation's 5G communications network and the European Supply Center, Huawei's largest facility outside of China which functions as a research and development institute for artificial intelligence, employing both Hungarian and Chinese scientists and technicians. The relationship's historical manufacturing aspect has also endured to the present day with Chinese companies such as BYD running factories for electric metropolitan buses for use in Budapest as well as potential future automotive manufacturing ambitions. Such results have an impact beyond Hungary's borders. It's development of its logistical and manufacturing capacities, along with its geographical location intersecting with numerous supplying and trading routes spanning from the Mediterranean to the steppes of Eurasia, position the country to be a key logistical node linking the East and the West; a position yielding both national pride and profit for the small nation. While such developments have greatly advanced Hungary's standing in technological modernization, such advancements have come with issues concerning security that have proven to be an elephant in the room that is becoming harder and harder for Budapest to sidestep.

Concerning Hungary's membership in NATO, the reliance on Chinese technology for 5G networks presents a problem in the minds of Europe's security officials. Concerns include the usual fears of espionage, which have already been well-documented and substantiated. However, there is also a growing fear of potential kinetic utilization of cyber-augmented infrastructure. Hungary's growing reliance on technology is a common phenomenon in Western nations. In the case of Hungary, this includes assets beyond telecommunications and into the realm of critical functions in logistics such as the East-West Intermodal Gate, research and development initiatives through institutes like the European Supply Center, and emergency services infrastructure with the Chinese-build communications system for the nation's first responders. Investment into such sectors has bred hypothesis among security-focused officials and analysts that China may possess the ability to either cripple Hungarian state-level functions or manipulate it to their own benefit. This supposition has led to a call for Hungary to abandon such infrastructure and to cut its technologically focused ties with China.

Hungary has expressed reluctance in following the trend of other European nations in cutting relations with Chinese technology companies.[4] Its political leadership has stated that it sees little evidence of a security risk and thus intends to continue the relationship. The dismissal of security concerns by political leadership has created tension and distance between Budapest and other nations of the European Union as well as the U.S. on security matters. From a disposition based on only publicly available information, the current strained relations seem to be based on the potential for danger rather than the evidence of it, at least in the context of Chinese-Hungarian relations. Whether these fears have actual merit to them will be explored in this report.

Chinese Cyber-Augmented Infrastructure Projects in Hungary[5]

China has several major projects and significant assets invested in Hungary across multiple sectors. Several projects collectively worth billions of euros have resulted from this growing partnership. Hungary plays a vital role in China's vision for the Belt and Road Initiative (BRI) linking east and west as a vehicle for Chinese exports to Europe. As such, Chinese projects in Hungary focus predominantly on industrial, digital, and logistical infrastructure. Specifically, the development of AI-augmented infrastructure has primarily taken form in manufacturing and telecommunications assets.

Given China's status as the world's largest industrial exporter and the centrality of logistics to the Belt and Road Initiative, most Chinese projects in the country are logistics-oriented. Budapest is the proposed terminus for a massive railway development poised to link Chinese-built logistical facilities in Hungary with the Chinese-owned port of Piraeus in Greece. The first leg alone will run for 350 kilometers from Budapest to Belgrade and cost some $2.89 billion. From Belgrade, the route will continue through Skopje and Athens to the Aegean Sea.[6] In anticipation of this new rail traffic, Hungary and China signed a land grant contract allowing Tonglinada, a Chinese logistics company, to develop a new China-Europe Logistics Trade Center in Budapest. The new 100,000 square meter facility is predicted to process over four million tons of goods per year and is scheduled to begin operations in 2024. At its fastest, this new Budapest route will reduce transit time by 7 days compared to current routes and allow goods to be delivered from Budapest to many regional hubs and ports in just 2-3 days.[7]

China already has several logistics and trade centers operating within Hungary as of 2023. China's East-West Gate Intermodal Terminal, heralded as the "western gate of the new silk road," opened in 2022 in Fényeslitke.[8] The terminal incorporates rail transit, road transit, transfer, and warehousing facilities with a capacity of handling one million TEUs per year. The terminal works in partnership with Kazakh rail freight operator EuroTransit, which has terminals at the Chinese-Kazakh border.[9] China has also invested some 200 million euros in the Central European Logistics and Industrial Zone near the town of Záhony. The project includes logistics, warehousing and intermodal transportation facilities to capitalize on planned upgrades to the Ukraine-Hungary wide-track reloading port.[10] The war in Ukraine is currently holding up transshipment from the Far East with the destruction of rail sections between Russia and Ukraine.[11] Hungary has even partnered with Chinese airports to become the airfreight hub of BRI. Budapest has signed agreements with China's Xi'an Xianyang and Zhengzhou Xinzheng Airports and established a special terminal at Budapest's airport exclusively for Chinese airfreight. Furthermore, a logistical subsidiary of China's Alibaba company announced Budapest as its "East and Central European Distribution Hub" with five scheduled air cargo services per week that resulted in an estimated 30% increase in cross-border e-commerce volume between Hungary and China in 2021 alone.[12]

In addition to logistics, China has also invested heavily in developing digital infrastructure projects in partnership with Hungary. Chinese telecommunications company Huawei has been a major partner in the development of Hungary's 5G network, alongside British and German firms Vodaphone and Telekom respectively.[13] Huawei has also built hardware for Hungary's emergency services, including a "unified emergency call system" linked to "internal radio systems" for police, fire, and medical teams.[14] Huawei has even launched its Seeds Scholarship Program in Europe at several Hungarian universities. The program, which recently expanded to Budapest's University of Public Service, focuses on "research and innovation related to 5G," according to Péter Szijjártó, Hungary's Minister of Foreign Affairs and Trade.[15]

Investments in digitalization have also gone hand-in-hand with China's logistics projects. The aforementioned East-West Gate has become the "world's first smart 5G railyard" thanks to Huawei technology. The facility boasts artificial intelligence-operated cranes, real-time cargo tracking, and high-speed wireless remote control over the entire container terminal zone.[16] Huawei also runs the European Supply Center in Páty, a 5G-integrated warehouse. The facility is at the center of the company's efforts to use 5G and "artificial intelligence-controlled image processing" to digitize logistical functions, manufacturing, and quality control tasks. It also boasts such automation methods as autonomous forklifts.[17]

China has even invested directly into industrial ventures in Hungary, most recently in automotive battery production facilities. Chinese battery maker Contemporary Amperex Technology Co. Ltd. invested $7.6 billion in a new factory in Debrecen. The factory would work with other automotive manufacturers already in Hungary including Mercedez, BMW, and Volkswagen.[18] A second Chinese company, Eve Power Co., is planning to build a battery factory in the same city worth approximately one billion euros. In response, BMW announced its own plans to construct an automotive plant in Debrecen also worth approximately one billion euros.[19] China's BYD automotive company is also anticipated to build its first European car plant in Hungary. In October 2023, Hungarian Prime Minister Viktor Orbán met with company executives and toured a BYD factory, and a concurrent BYD statement said that the company was "looking for a suitable location" for the new plant.[20] BYD already has an electric bus plant in Komárom, Hungary that opened in 2017. By 2022, the plant had a yearly production capacity of 1,000 buses and some 16.3 million euros invested. For perspective, anticipated Chinese total direct investment in Hungary for 2023 was 13 billion euros, doubling their investments in 2022.[21]

China perceives Hungary as one of its primary trade gateways into Europe and an important part of the Belt and Road Initiative and has taken steps to realize this vision through trade, digital infrastructure, and industrial investments. Industry, trade, and transport (alongside accommodation and food services) collectively comprise some 41.2% of Hungary's economy.[22] This means that China's involvement in these sectors presents great potential, but also great potential risk. In addition, Chinese involvement in Hungary's 5G network and emergency service infrastructure has

meant a leap forward for digitalization efforts, but creates a further risk for disruption, interference, or surveillance if relations between these countries sour. Either way, China is a major partner for Hungary and vice versa (at least in Europe), and the current administration in Budapest shows no signs of changing course on Chinese relations in the foreseeable future.

Potential Chinese Actors and Motivation[23]

The infrastructure established in Hungary by Chinese entities has the potential to be utilized for malicious purposes by varying levels of Chinese authorities and organizations. The motivation of national-level leadership is most likely to be oriented towards Hungary's international political, security, and economic relations with NATO and the European Union rather than Hungarian institutions. Actions may also be undertaken by various clans and organizations within the Chinese Communist Party for either their own economic or political objectives that do potentially target Hungarian assets, with or without the guidance and consent of Chinese national leadership.

With Sino-Hungarian relations being characterized as "a model of international relations" by CCP Politburo Foreign Relations Director Wang Yi,[24] the Budapest relationship has proven to be an asset for the Chinese government. Thus, any centrally-guided Chinese operations that would maliciously use digital structures in Hungary are unlikely to be aimed at damaging Hungarian institutions. Instead, such operations may use Hungarian structures as a bridgehead into the EU and NATO to target more strategically important Western assets or drive a wedge between the United States and the EU. However, if malicious Chinese operations in Hungary were not centrally guided, or only partially so, they could be driven by a more comprehensive array of actor types and motives. Finally, miscalculations can cause the Chinese party-state to sacrifice the excellent relationship and trust it has built up with the Hungarian government.

Hungary: An Unlikely Primary Target

Hungarian state institutions are unlikely to be prime targets in China's primary strategy toward Europe. If cyberattacks, espionage, or other malicious actions by centrally-guided Chinese players would involve assets and infrastructure in Hungary, it is more likely that their strategic use will be that of providing a bridgehead into the EU and NATO. China's apparent grand strategy—disrupting or diluting the US-EU alliance vis-à-vis China—will be discussed in the next section. Hostile actions targeting Hungarian institutions are unlikely to be part of that grand strategy, first, because maintaining good relations with Hungary is valuable to China as the close Hungarian-Chinese diplomatic relationship offers China a foothold in the political landscape of the wider EU sphere. Second, Hungary itself is not strategically important enough to be the primary end target of a possibly malicious Chinese strategy toward Europe.

As of writing, Sino-Hungarian diplomatic relations are warm, with China's increased activity in Hungary swimming against the stream in the EU. Whereas the European Commission's doctrine is "derisking,"[25] "connectivity" is the buzzword of the Hungarian government.[26] Since 2010, the Hungarian government has sought to increase connectivity with the People's Republic of China through Hungary's ascension to the Asian Infrastructure Investment Bank (AIIB) and with policy strategies such the "Opening to the East" which promote hosting Chinese ventures such as the Belt and Road Initiative.Budapest's continuous efforts at outreach while other Western states and the EU became more hesitant has positioned Prime Minister Victor Orbán as "the very last friend of Beijing in the whole of the EU," as characterized by Tamas Matura, an international relations scholar at Budapest's Corvinus University.

In October 2023, Prime Minister Orbán was the only national leader of a Western or EU country who was in Beijing to attend the Third Forum of the Belt and Road Initiative (BRI). Hosted by General Secretary Xi Jinping, this forum commemorated the tenth anniversary of the BRI, an infrastructure development umbrella linking China to other world regions and Europe, particularly in fields such as trade and construction. Though eighteen EU countries signed a memorandum to be part of the BRI at some earlier point, only Hungary sent a high-level delegation to the Third Summit. While in China, Prime Minister Orbán was rewarded with meetings with high level officials including CCP General Secretary Xi, Chinese Premier Li Qiang, the chairmen of four of China's largest banks, and Ren Zhengfei, the founder-chairman of telecommunications giant Huawei.[27]

As a demonstration of China's success at garnering affinity in Hungary, the sentiments of the general population have been the least negatively disposed toward China out of the nine EU member states polled by Pew.[28] Half of the Hungarian respondents were "unfavorable" toward China, while 42 percent were "favorable," a less negative score than measured elsewhere in the Western world. Matura assesses that the less Sinoskeptic mood among the Hungarian public is due to the government's Sinophilic policies and rhetoric "shaped a pro-China narrative in national governmental communication and pro-government media outlets. … The outcome of these governmental communication efforts was a sharp increase in China's reputation among voters of Fidesz, the nation's ruling political party."[29]

Regardless of whether this causal connection postulated by Matura is accurate or not, the relative popularity that China enjoys in Hungary, the business connections (outlined in the previous chapter of this report), and the diplomatic connectivity all add up to a substantive asset. For the Chinese government, there is thus objective value in maintaining its outstanding diplomatic relationship with Hungary, which is one reason why damaging Hungarian institutions is unlikely to be the direct, primary target of potential Chinese cyberattacks, espionage, or other malicious actions in Hungary and the EU.

Another reason, as mentioned, is that Hungary would not be strategically valuable enough to be the prime target of malicious actions by a geopolitical player of the People's Republic. Hungary is a small country with ten million inhabitants and an economy that is heavily intertwined with that of Germany's which has a nominal GDP is 23 times larger in absolute terms and roughly three times larger per capita.[30] In the Global Innovation Index of 2022, Hungary ranks 34th globally and 22nd within the European region with a score of 39.8, while China ranks 11th globally with a score of 55.3.[31] In the US News ranking of "Most Influential Countries," Hungary is 43rd, while China is in second place.[32] In conclusion, it is unlikely that any potential Chinese cyberattack, espionage, or other malicious action committed to further the central Chinese party-state's primary strategic goal toward Europe would have a Hungarian-centered final objective.

The CCP's Primary Strategic Goal in Europe: EU Political and Economic Divergence from the US

If Hungarian institutions were to be targeted by Chinese cyberattacks, espionage, or other malicious actions, those attacks would likely be driven by other motives or actors other than the central leadership of the party-state in Beijing, i.e., the Politburo of the Chinese Communist Party (CCP). Instead, such actions would be deriving from lower-level Chinese actors in politics or business (see the discussion of actors in the next segment); or, if ordered by the political center, they would seek to utilize Hungarian infrastructure as an access point into the EU or NATO. Hungary could serve as a lever for breaking open these alliance formations.

In theory, using compromised Hungarian structures as a beachhead into the EU and NATO could potentially serve what appears to be China's primary strategic goal toward Europe: to drive a wedge between the United States and the EU in their collective political stance towards China. This could theoretically prevent the formation of an anti-Chinese Western block. When standing united, the EU and the US are a formidable force in global geopolitics (though as a negative to the EU, this unity may entail either a perceived or actual subordination of EU interests to those of the US). In contrast, a more geo-strategically pluralized or divided West would allow China to develop more amicable relations with the EU and leave more room for strategic maneuvering toward the US. In particular, the Chinese party-state is fearful of and motivated to undercut the Biden administration's tech offensive against China. The Biden administration attempts to mobilize allies in limiting Chinese access to advanced computing silicon chips, supercomputer technology, advanced semiconductors, and machines for making semiconductors, such as the extreme ultraviolet lithography machines issued by Dutch tech giant ASML.[33]

The evidence that encouraging Western sub-differentiation or division (also known more positively as European "strategic autonomy," 战略自主, *zhànlüè zìzhǔ*[34]) is indeed the primary strategic goal of the Chinese party-state's center are statements by Chinese politicians, statements concerning Chinese strategy by EU or EU member state politicians, and independent expert assessments. Von der Leyen, President of the European Commission, has previously accused China's government of trying to divide the EU on China. On a state visit to Beijing in April 2023, Von der Leyen stated, "We have already, in the recent days and weeks, seen those tactics in action."[35] She reminds us, "A strong

European China policy relies on strong coordination between member states and EU institutions, and on a willingness to avoid the divide and conquer tactics that we know we may face." This desired unity however has proven to be contested. President Macron of France, whose mission to Beijing Von der Leyen joined, stressed that, though union within the EU is essential, the EU and EU member states should be able to think independently from the US on issues relating to China. "We Europeans must wake up. Our priority is not to adapt to the agenda of others in all regions of the world." He argues for a "European strategy," which was music to the ears of their Chinese host, who has been encouraging such an EU-European strategic autonomy. As documented by the Germany-based Mercator Institute for China Studies (MERICS), Chinese politicians and diplomats have expressed hope that the EU realm will pursue a "third way" (第三条道路, *dìsān tiáo dàolù*) that diverges from America's stances on China.[36] Xi Jinping, General Secretary of the CCP, argued in 2021 that "China's development is an opportunity for the European Union; we hope that the EU will make correct judgments independently (from the US) and truly realize strategic autonomy" (中国发展对欧盟是机遇, 希望欧盟独立作出正确判断，真正实现战略自主, *Zhōngguó fāzhǎn duì ōuméng shì jīyù, xīwàng ōuméng dúlì zuòchū zhèngquè pànduàn, zhēnzhèng shíxiàn zhànlüè zìzhǔ*).[37]

Possible Actors: The Center, Clans, and Business

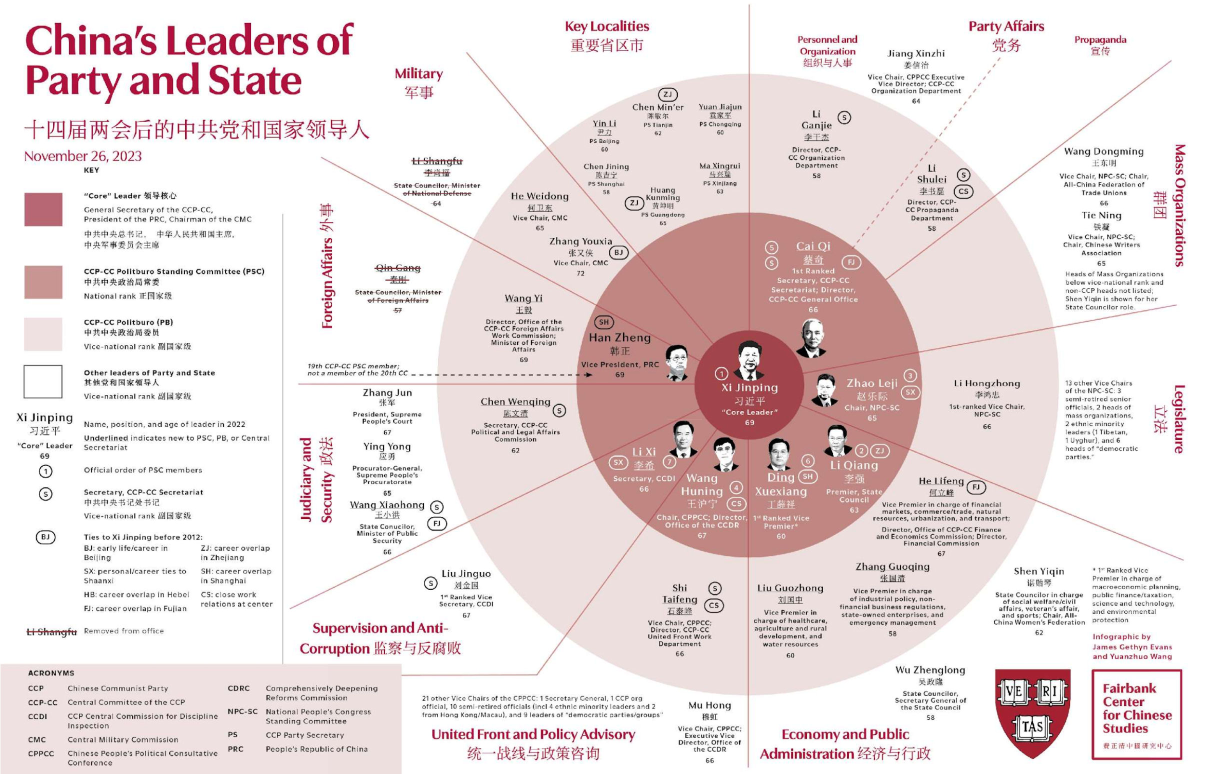
Significant operations that either further or risk China's primary strategic goal in Europe may require clearance from the political center. This political center is represented in the first instance by General Secretary Xi, the "leadership core" (领导核心, Lǐngdǎo Héxīn), then by the Standing Committee of the CCP-CC Politburo and following that, the Politburo in its entirety. However, malicious actions such as cyber attacks and espionage can also originate from other positions inside the Chinese party-state or even from Chinese business actors. Such a peripheral or pluralistic origin is more likely when operations are less significant in scope or do not pose a potential risk to the center's grand strategy. Operations can run through the formal state channels in a top-down manner, but be nonetheless decentralized in the sense of being directed from outside of Beijing. *The Financial Times* reports that Nigel Inkster, the former operations head at MI6, "said the MSS [China's Ministry of State Security] conducted most of its espionage through provincial departments and Zhejiang had 'primacy' for operations in Europe."[38]

The question as to which level an operation ultimately originates is likely to be unclear to external observers basing their analysis on the public record, even if an operation were to have been shown to have occurred. Take the example of the two recent hits on Dutch tech giant ASML, which produces the prized extreme ultraviolet lithography machines and has become a football in the US-Chinese tech rivalry. In the first instance in 2022, a Chinese employee stole trade secrets from ASML and later resurfaced at tech giant Huawei, Dutch newspaper NRC reports.[39] Also in 2022, ASML accused the Chinese company Dongfang Jingyuan Electron of stealing trade secrets in a seemingly separate incident.[40] Based on publicly available information, it is impossible to determine whether one or both of these attacks against ASML had clearance from the center of the Chinese leadership. Such a situation is not impossible given the company's strategic importance to the American tech embargo that China fears and against which its grand theory in Europe appears to be aimed.

A complicating factor is that the CCP, let alone the party-state, is far from a monolith. It regionally subdivides, with regional departments such as the Ministry of State Security in Zhejiang, which fields an estimated five thousand intelligence officers[41], playing an active and possibly fairly autonomous role in relation to Europe.[42] Also, the party-state comprises clans, factions, and networks that intersect with and run through different regions and levels of state and party organizations. Since this clannism is informal, largely hidden, and complex, identifying the actor behind party-state operations is exceedingly challenging. Initiatives may come from the center, pretend to come from the center, be co-opted by the center, or originate from ten thousand other sources.

Unless General Secretary Xi is directly and explicitly involved, it is often unclear, even in theory, who or what represents the center. Instead of evident and stable, association with the center is aspired to, competed over, constantly shifting, and often ambivalent. This association is a type of political capital fought over, accrued, and employed instrumentally, as theorized by French sociologist Pierre Bourdieu's model of the "field of power" in socialist party-state systems.[43] Even scholars in Chinese academia sometimes seek to give weight to their postulations by claiming to transmit "Xi Jinping Thought" and offer better interpretations than scholarly rivals, which is the academic version of politicians claiming legitimization from the political center.[44]

Though the clannism within party-state structures is hidden from the view of outsiders, it is prevalent based on extrapolations from expert observations of clannism in the broader Chinese society and from incidental breakdowns in the outer appearance of internal party unity. In *The Party: The Secret World of China's Communist Rulers* (2010), *The Financial Times'* former China bureau chief Richard McGregor provides a topology of the Chinese party-state. Due to the system's opaqueness and internal orientation, its composition into factions and clans only comes to the surface in rare incidents in which conflicts spiral out of control: "Once in a while there was hard evidence of conflict, as the casualties of corruption scandals, factional clashes or plain mismanagement were thrown out into the street, to be carted off into retirement or prison."[45] For example, in 2012 and 2013, we learned that Politburo Standing Committee member Zhou Yongkang was the patriarch of a clan including Bo Xilai, the Communist Party Secretary of Chongqing, when both men were purged by factions favorable to the incoming paramount leader Xi. More recently, Qin Gang, State Councilor and Foreign Minister, and Li Shangfu, State Councilor and Defence Minister, as well as some of their underlings, disappeared in the same period, leading to speculation that they may have been part of a purged clan. Their names are crossed out in the below chart of the formal structures of China's party-state center published by Harvard's Fairbank Center on November 26, 2023.


China's Leaders of Party and State
十四届两会后的中共党和国家领导人
November 26, 2023
KEY
"Core" Leader 领导核心
General Secretary of the CCP-CC, President of the PRC, Chairman of the CMC
中共中央总书记、中华人民共和国主席，中央军事委员会主席
CCP-CC Politburo Standing Committee (PSC) 中共中央政治局常委 National rank 正国家级
CCP-CC Politburo (PB) 中共中央政治局委员 Vice-national rank 副国家级
Other leaders of Party and State 其他党和国家领导人 Vice-national rank 副国家级
Xi Jinping 习近平 "Core" Leader 69
Name, position, and age of leader in 2022
Underlined indicates new to PSC, PB, or Central Secretariat
1 Official order of PSC members
S Secretary, CCP-CC Secretariat 中共中央书记处书记 Vice-national rank 副国家级
BJ Ties to Xi Jinping before 2012:
BJ: early life/career in Beijing
ZJ: career overlap in Zhejiang
SX: personal/career ties to Shaanxi
SH: career overlap in Shanghai
HB: career overlap in Hebei
CS: close work relations at center
FJ: career overlap in Fujian
~~Li Shangfu~~ Removed from office
ACRONYMS
CCP Chinese Communist Party
CCP-CC Central Committee of the CCP
CCDI CCP Central Commission for Discipline Inspection
CMC Central Military Commission
CPPCC Chinese People's Political Consultative Conference
CDRC Comprehensively Deepening Reforms Commission
NPC-SC National People's Congress Standing Committee
PS CCP Party Secretary
PRC People's Republic of China
Military 军事
Key Localities 重要省区市
Party Affairs 党务
Personnel and Organization 组织与人事
Propaganda 宣传
Mass Organizations 群团
Legislature 立法
Economy and Public Administration 经济与行政
United Front and Policy Advisory 统一战线与政策咨询
Supervision and Anti-Corruption 监察与反腐败
Judiciary and Security 政法
Foreign Affairs 外事
~~Li Shangfu 李尚福 State Councilor, Minister of National Defense 64~~
He Weidong 何卫东 Vice Chair, CMC 65
Zhang Youxia 张又侠 BJ Vice Chair, CMC 72
ZJ Chen Min'er 陈敏尔 PS Tianjin 62
Yin Li 尹力 PS Beijing 60
Yuan Jiajun 袁家军 PS Chongqing 60
Chen Jining 陈吉宁 PS Shanghai 58
Ma Xingrui 马兴瑞 PS Xinjiang 63
ZJ Huang Kunming 黄坤明 PS Guangdong 65
~~Qin Gang 秦刚 State Councilor, Minister of Foreign Affairs 57~~
Wang Yi 王毅 Director, Office of the CCP-CC Foreign Affairs Work Commission; Minister of Foreign Affairs 69
19th CCP-CC PSC member; not a member of the 20th CC
SH Han Zheng 韩正 Vice President, PRC 69
1 Xi Jinping 习近平 "Core Leader" 69
S S Cai Qi 蔡奇 FJ 1st Ranked Secretary, CCP-CC Secretariat; Director, CCP-CC General Office 66
Zhao Leji 赵乐际 3 SX Chair, NPC-SC 65
2 ZJ Li Qiang 李强 Premier, State Council 63
6 SH Ding Xuexiang 丁薛祥 1st Ranked Vice Premier* 60
Wang Huning 4 王沪宁 CS Chair, CPPCC; Director, Office of the CCDR 67
SX Li Xi 李希 7 Secretary, CCDI 66
Li Ganjie S 李干杰 Director, CCP-CC Organization Department 58
Jiang Xinzhi 姜信治 Vice Chair, CPPCC Executive Vice Director; CCP-CC Organization Department 64
Li Shulei S 李书磊 CS Director, CCP-CC Propaganda Department 58
Wang Dongming 王东明 Vice Chair, NPC-SC; Chair, All-China Federation of Trade Unions 66
Tie Ning 铁凝 Vice Chair, NPC-SC; Chair, Chinese Writers Association 65
Heads of Mass Organizations below vice-national rank and non-CCP heads not listed; Shen Yiqin is shown for her State Councilor role.
Li Hongzhong 李鸿忠 1st-ranked Vice Chair, NPC-SC 66
13 other Vice Chairs of the NPC-SC: 3 semi-retired senior officials, 2 heads of mass organizations, 2 ethnic minority leaders (1 Tibetan, 1 Uyghur), and 6 heads of "democratic parties."
He Lifeng 何立峰 FJ Vice Premier in charge of financial markets, commerce/trade, natural resources, urbanization, and transport; Director, Office of CCP-CC Finance and Economics Commission; Director, Financial Commission 67
Zhang Guoqing 张国清 Vice Premier in charge of industrial policy, non-financial business regulations, state-owned enterprises, and emergency management 58
Liu Guozhong 刘国中 Vice Premier in charge of healthcare, agriculture and rural development, and water resources 60
Shen Yiqin 谌贻琴 State Councilor in charge of social welfare/civil affairs, veteran's affair, and sports; Chair, All-China Women's Federation 62
* 1st Ranked Vice Premier in charge of macroeconomic planning, public finance/taxation, science and technology, and environmental protection
Wu Zhenglong 吴政隆 State Councilor, Secretary General of the State Council 58
Mu Hong 穆虹 Vice Chair, CPPCC; Executive Vice Director, Office of the CCDR 66
Shi Taifeng S CS 石泰峰 Vice Chair, CPPCC; Director, CCP-CC United Front Work Department 66
21 other Vice Chairs of the CPPCC: 1 Secretary General, 1 CCP org official, 10 semi-retired officials (incl 4 ethnic minority leaders and 2 from Hong Kong/Macau), and 9 leaders of "democratic parties/groups"
S Liu Jinguo 刘金国 1st Ranked Vice Secretary, CCDI 67
Chen Wenqing 陈文清 S Secretary, CCP-CC Political and Legal Affairs Commission 62
Zhang Jun 张军 President, Supreme People's Court 67
Ying Yong 应勇 Procurator-General, Supreme People's Procuratorate 65
Wang Xiaohong S 王小洪 FJ State Conucilor, Minister of Public Security 66
Infographic by James Gethyn Evans and Yuanzhuo Wang
VE RI TAS
Fairbank Center for Chinese Studies
費正清中國研究中心

Graph: "China's Leaders of Party and State," Harvard's Fairbank Center, 26 Nov. 2023

The existence of clannism in the CCP and the party-state can be extrapolated from social scientific knowledge on the importance of clannism in the broader Chinese society and business in particular. Neo-institutionalist approaches in organizational sociology stress the powerful effects of "institutional isomorphism," which is the converging of different institutional fields across a polity, as first theorized by DiMaggio and Powell in their famed paper "The Iron Cage Revisited."[46] The implication is that isomorphic pressures render it probable that values and styles of organization found in Chinese business will resemble those in Chinese politics, despite all the differences between business and politics. As documented in the academic literature, "guanxi," which is social networking capital, is central to status dynamics and socializing in Chinese business. Sociologist Bian Yanjie discusses its various definitions.[47] In one meaning, "guanxi is the web of extended familial obligations; guanxi capital accumulates when one invests time and energy to extend the ties of familial sentiments and obligations."[48] In another, guanxi is "a type of social-exchange network of asymmetric transaction."[49] Guanxi networks are informal, hierarchically structured, family-like dependencies from which social capital can be mobilized across locales, societal fields, and organizational levels, crosscutting formal institutions in clannish ways. These guanxi networks, observed in business, are perhaps as prominent in politics, as Guo Xuezhi argues in "Dimensions of Guanxi in Chinese Elite Politics."[50] In fact, guanxi-driven, clan-like networks with the highest social capital are precisely those that connect leaders in politics and business and thus cross over into both fields.

A final point of complexity is that the actors pursuing an operation can change midway through the operation, for example, when political power-holders reprimand business networks, or a lower-level administration or less powerful clan is exposed, sidelined, demoted, or scapegoated by a higher or more powerful one. In mainland China, every major institution or organization in administration, politics, education, journalism, or the economy, including every mid to large private company, has an official party cell that can be activated during conflict or crisis. In addition, board members will often be party members, further cementing the embedding of corporate business in party structures.

Illustrative of how the party elements in private companies tend to be determinative, private companies based in China can be taken over from within by political players and concerns even when they are (partly) foreign-owned. Such an internal take-over occurred with Sanlu, the prime culprit in the 2008 Chinese milk scandal. Sanlu was owned for 43 percent by the New Zealand dairy cooperative Fonterra. When Fonterra's representative in Sanlu's board heard on August 2, 2008, that Sanlu had become aware that its baby formula was contaminated with harmful doses of melamine, Fonterra argued for a public recall of all Sanlu products. However, under the instruction of the Shijiazhuang municipal government, party members in Sanlu's board sought to lift the scandal over the 2008 Beijing Summer Olympics, which were to commence on August 8. New Zealand's Fonterra had lost all influence in the Sanlu board. Even in September, after the Olympics, Fonterra had been so cut off from Sanlu's management that it had to reach out via New Zealand diplomats. Only after these diplomats had contacted China's central government about the problem with Sanlu and Shijiazhuang, Sanlu recalled all its contaminated products.[51] Several Shijiazhuang officials were forced to resign. The scandal's trajectory shows how fissures can appear between foreign business entities and Chinese, party-embedded business people, and between the center and local levels of administration in the party-state.[52]

Extrapolating from this insight, it is possible to imagine a scenario in which a private Chinese company would undertake espionage or commit a cyber-attack in Hungary for strictly commercial reasons, only to be taken over "from within" by a party cell, political faction, or the political center when Chinese politicians start seeing the operation or entity in question as somehow politically relevant (for example, as a political risk or opportunity). This possibility of a switch of actors in the background, alongside the other complicating factors (including hybrid guanxi networks and the ambivalence and contested character of claims to the central Chinese line), all contribute to—but do not exhaust—the complexity of the question of actors.

Risk of Miscalculation and International Crisis

Finally, due to miscalculations, centrally guided Chinese operations could damage Hungarian interests and the Sino-Hungarian diplomatic relationship despite this relationship currently constituting a substantial asset to Beijing. The risk of fateful miscalculations is especially pronounced in Chinese foreign policy because the CCP is an apparatus with around a hundred million members that soaks in its own information environment. Large organizations, like great powers and empires, tend towards self-absorption, as scholar of geopolitics Edward Luttwak argued in his 2013 book *The Rise of China vs. the Logic of Strategy*.[53] In China, tendencies toward self-absorption are further intensified by the massive censorship and propaganda apparatus of the party state, the size of the Chinese population, and linguistic barriers. Self-absorption increases the risk of misunderstanding geopolitical situations and other player's motives, which, in turn, raises the risk of unnecessarily harming valuable relations, such as the Sino-Hungarian one, through reckless, misguided, or mistimed actions.

An example of such a strategic error by the Chinese government deriving from an apparent inability to anticipate the other side's political process is China's response to South Korea's 2016 announcement that it would deploy THAAD (Terminal High Altitude Area Defense), which is an American anti-ballistic missile defense system. The United States military supplied this system to South Korea to shield it from North Korean rockets. Still, the strategic position of the Chinese government was jeopardized (there is ongoing discussion about why this was[54]). After Seoul acquired THAAD despite complaints and warnings from Beijing, Beijing installed informal boycotts on Korean cultural products, cooperations, and businesses in mainland China.

Ironically, shortly before, Seoul had seemed to be reaching out to Beijing, thereby worrying Washington; for example, Korean President Park Geun-hye had attended the 2015 China Victory Day Parade in Beijing. However, Beijing's "bullying power politics," in the words of Pusan-based international relations scholar Robert E. Kelly[55], backfired, pushing Seoul closer to Washington and alienating the South Korean public. That it backfired should not have been surprising, yet, tellingly, many Beijing observers appear to have been caught off guard. To illustrate, in a Zoom interview with Ph.D. researcher Phoebe Moon on January 23, 2022, Korean parliamentarian Kim Youngho reports that a Chinese academic interlocutor in 2017 had been "dumbstruck" by his suggestion that China's attempts at coercion alienated South Koreans and further pushed Seoul toward Washington in security matters.[56]

Hence, it is entirely possible that a miscalculation of political dynamics in the EU and Central Europe could prompt the central leadership in Beijing to act on poor strategy, consequently jeopardizing or losing its assets or influence in Hungary or counter-productively creating a backlash that defeats the purpose of an operation. In a future scenario, China may overplay its hand when offensively activating its structures in Hungary. It could underestimate the public backlash, EU unity, or Western resolve or overestimate how much its assets and structures in Hungary can function as a beachhead for more comprehensive operations. In the process, it may damage its European assets, Sino-Hungarian relations, Sino-EU relations, and concrete economic and organizational structures vital to Hungarian society. In conclusion, the connectivity with Hungary enables the Chinese government and its Belt and Road Initiative to reach deeply into the EU (and into a NATO country), which is potentially of great strategic value, economically and politically, when handled with discernment and prudence; yet, it is to be seen if Beijing and Budapest will manage to reap the rewards of their mutual outreach in the hectic geopolitical environment of the twenty-first century.

Artificial Intelligence, Automation vs Artificialization, and the Agential Indiscernibility Problem[57]

Chinese-built Hungarian infrastructure that utilizes artificial intelligence provides an ideal tool of malicious intent due to the utility of AI in automated asset management of assets as well as the incredible difficulty in determining its origins. The rapid development of AI capabilities has resulted in a general understanding of what AI is and what it is capable of in near constant fluctuation.

Amidst the transformative shift of the ongoing AI revolution, and the rapid expansion of the frontier of technological possibilities to an extent that is not currently known, it is critical to consider the role played, or the role that might be played, by AI in the landscape of Chinese FDI in Hungary.

Merely two years ago, any discussion on the topic of cyber capabilities possessed by a foreign state actor would have looked very different. In 2021, it was feasible to discuss cybersecurity threats posed by foreign states, the sophistication of their offensive and defensive capabilities, and the potential countermeasures that could be implemented for mitigation purposes, with a degree of certainty that was at least proportional to the quality and quantity of information available to the discussants. At present, this is no longer the case.

This sudden and dramatic disappearance of precision and certainty in cybersecurity studies has been caused by the advent of a novel technological development that appears poised to effect a full-scale transformation of economic processes across the globe. We are referring, of course, to artificial intelligence (hereafter, AI). As of now, the topic of AI is fully embedded into every relevant conversation or strategic consideration in the fields of cybersecurity and cyber warfare. It is inescapable, and omnipresent.

It is important to recognize, as a caveat, that cybersecurity does not intrinsically or necessarily involve AI as one of its core components. For instance, the Pegasus spyware system developed by Israeli intelligence services,[58] used to hack into smartphones through zero-click exploits that have cross-OS compatibility, is widely accepted to be the most advanced offensive cyber capability to have emerged during the previous decade (at least, among those that are publicly known).[59] This pre-AI tool was used to devastating effect by Israeli intelligence operatives throughout the 2010s, and stands as an example of the sophistication of offensive cyber warfare to this day.[60] On the other hand, there is a strong and obvious incentive for state actors to enhance extant cyber capabilities like Pegasus by retrofitting them with the new possibilities introduced by AI in 2022 - an incentive already explored in the case of the Pegasus System, which is reported to have received such retrofitting back in 2023.[61] As such, it must be recognized that cybersecurity in the current year cannot ignore AI, in concept or in application. With new moves now allowed on the chessboard, it is inconceivable for a grandmaster to carry on as if playing a regular game of chess.

What is AI?

Within recent memory, artificial intelligence (AI) went from a science fiction trope to one of the most overused (and least understood) phrases in media and society virtually overnight. The overuse (and misuse) of the term creates many problems, among which the lack of clarity and conceptual understanding is perhaps the most salient. As a cursory internet search will immediately reveal, the definitional boundaries for AI are hotly contested.[62] A plethora of definitions backed by different sources compete against one another for legitimacy and credibility, often having rival agendas behind them.[63] We propose to ignore this semantic anarchy entirely by discussing AI in simple, commonsensical terms that are universally agreed upon.

In the broadest possible sense, AI describes systems, technologies, and processes that accomplish goals and tasks using adaptive logic, rather than procedural logic.[64] Whereas a standard computational process (SP) might respond to an input by following a simple, pre-programmed decision tree, moving from 1, to 2, to 3, et cetera, an artificially intelligent process (AIP) would treat each step as a discrete interval at which to pause and calculate a contextually appropriate solution before moving forward. Simply put, an SP responds to inputs as instructed by its programming such that it generates outputs which are predictable and static, whereas an AIP responds adaptively at every stage of the problem-solving process,[65] making no two outputs the same while simultaneously dramatically exacerbating the difficulty of predicting outputs at any given stage of computational processing.[6667]

AI vs Automation in Economic Cyber Warfare

The phenomenon of automation (the replacement of human labor by industrial processes that do not require active human input or management) is highly significant in political and economic contexts.[68] Automation is an established political issue in the United States, where candidates from both major parties such as Donald Trump and Andrew Yang have used it as a focal point to promote their own solutions and capture the attention of the electorate.[69, 70]

In addition to the United States, automation is also a fact of life in Hungary, where deindustrialization of the economy continues to accelerate, and those factories that remain or are under construction see increasing levels of labor-free automated production methods. Among the newer factories are those implementing novel methods of “AI-based production” such as the Bridgestone auto factory in Tatabánya.[71] The growing uptake of AI in manufacturing within Hungary, at production sites that are funded by FDI from states such as Japan and China,[72] increases the importance for analysts and policymakers to understand what the differences between automation and AI-based production are, including but not limited to manufactorial contexts.[73]

In the case of automation, i.e. in the context of a fully automated assembly line within a factory or manufacturing plant, the process is prescribed and pre-planned, involving predetermined steps that are carried out in sequence from A to Z, or from 1 to 10. Because of the predetermined and predictable nature of these automated processes, it is incredibly easy to detect, and thus address, any unwanted modifications of said process that might be introduced by a hostile actor in the cyber context. If a factory assembly line managed by a central computer were to suddenly change its behavior in any way, this would constitute an anomaly and therefore be immediately diagnosable as a threat.

AI-based manufacturing processes, on the other hand, are not inherently regular or predictable.[74] In such cases, where the very purpose of the system itself is to adaptively respond to changes in conditions that a human or automated program might fail to handle, each actionable stage within the production line is resolved by the system with a greater degree of freedom and flexibility than would otherwise be the case. A critically important consequence of this is that an artificially intelligent process in an industrial context is incredibly difficult, if not impossible, to interpret.[75] Because the expected behavior of an AI-based process (at any stage of production) is not predictable (unlike an automated production line) human agents overseeing these processes are forced to rely upon little more than gut instinct when determining whether the process is operating as expected, or instead being altered or interfered with by a hostile actor.[76]

Stepping back to look at these two processes, it should be clear why the two have dramatically different ramifications in the context of cyber-security and cyber warfare. Automated processes can indeed be hacked, altered, hijacked, and modified; this is not at all new or surprising. Artificially intelligent processes, by contrast, can be hacked, altered, hijacked, or modified in ways that are indistinguishable from outcomes that fall within the parametric limitations of the system's generic programming. The contrast between the two systems is not one of functionality, but of detectability and visibility.

This contrast, and more broadly also the transition from a system where industrial sabotage is understood to be identifiable into one in which salient actors acknowledge that it cannot even be perceived, constitutes what is arguably the most significant concern for Chinese industrial and cyber investments in Hungary (as well as the EU in general).

The Indeterminacy and Invisibility of Cyber Sabotage in the AI Age

Responding to threats by hostile actors, corporate, state, or otherwise, requires those responding to first detect the threat, then to determine the nature of the threat, and lastly to respond to it. If it goes undetected, or if the targets of a cyber attack are unaware that they are being attacked, none of these steps can take place, rendering self-defense impossible.

The most salient concern with regards to the implementation of AI-based systems in Hungary, taped together with FDI packages ostensibly intended to revitalize or bolster the local economy, is precisely this. AI-based systems and processes, in these contexts, intrinsically constitute what Donald Rumsfeld famously referred to as "unknown unknowns".[77] To understand why, it is helpful to draw upon a thought experiment. Consider a scenario in which a telecommunications network utilizing AI-based processes suddenly fails to deliver coverage to a localized area in Hungary. We are aware of what is happening, and we can quantify the degree to which it has an adverse effect, but we cannot know why it is happening in the first place. Is the process simply adapting to circumstantial developments we have yet to notice? Is it doing what it *ought to be doing*, at a time when we remain incapable of knowing what changes in the system require it to do so? Or is the system instead being weaponized as an offensive cyber capability by a hostile actor?

Fundamentally, the advent of AI-based production processes, as well as the retrofitting of these processes in other areas of the economy, have led to a situation where we can know what is happening, but not why. By virtue of having a hefty degree of freedom in responding to the task at hand, AI systems behave in ways that cannot be predicted, nor immediately explained. While a human factory worker could at any moment exhibit behavior that is anomalous and seemingly harmful, he can be questioned after the fact as to what rationale guided his actions, and what motivations he had in mind when committing himself to doing them. In the case of AI-based processes, this is not so.

When an AI-based process causes a catastrophic failure at a factory or industrial plant, it is impossible to objectively assess what calculations brought about this outcome, nor whether or not hostile actors played a role in creating it. If we take the most extreme example conceivable—an AI-based process causing an industrial accident that results in the loss of life—we are incapable of determining what the opportunity cost of the industrial accident was. Perhaps without this accident an even more serious disaster might have occurred, resulting in the destruction of the entire production facility, and the loss of many more lives. Or perhaps this accident was the consequence of a hostile actor utilizing AI infrastructure in offensive cyber warfare. What matters most is that, assuming the actions in question fall within the scope of the permutative outcomes the AI process *could have* produced, we are unable to verify why it behaved in this way.

Ultimately, *it is impossible to know* when and why an AI-based system misbehaves. Even in retrospect, there is no known means by which to conduct a 'digital autopsy' of this kind. With trillions of possible permutations for each decision at each stage of a production line allowed by the programming of an AI-based production process, the reality is such that cyber sabotage and hostile cyber attacks are in some cases indistinguishable from normal procedural behaviors of core industrial systems. This is what we define as the "Agential Indiscernibility Problem," which may ultimately prove to be a contingent limitation that will be resolved through further technological developments likely also invested into the improvement of AI capabilities. Whether the problem is contingent upon our current limitations or a more permanent fixture of our technological paradigm, the fact of the matter is that determining the agency behind an unexpected outcome resulting from any AI-based process is orders of magnitude more difficult than with the automated processes we are accustomed to – in some cases being in all respects functionally impossible.

Conclusion[78]

The greatest risk that Hungary faces concerning its relationship with China through its research and development of 5G telecommunications and artificial intelligence is its security alliances with the United States and Europe, primarily through NATO. The current political calculations by American and EU leadership in seeing China as a security risk by extension concern Hungary due to its relationship with China. Regarding potential actions that China may make with hostile or malicious intent, there are two levels of potential: ones implemented by national leadership, and those that are implemented by factions or clans with immediate local interests in Hungary such as business organizations and parties. These different levels, and their corresponding interests, are very likely to be pursuing different courses of action should their intentions turn malicious. Actions guided by national leadership will be focused on the larger strategy of instead targeting larger U.S.-European while using Hungary as an access point. Actions undertaken by specific clans or divisions within the Communist Party that are not guided by national leadership meanwhile are more likely to be focused on specific interests concerning business, which more directly focus on Hungary itself.

With these dynamics, two potential challenges exist for Hungary in the cyber domain: the degradation of its relations concerning cybersecurity with the rest of Europe and the U.S. and potential risks to its own infrastructure. The first risk is more likely to originate from an effort on the part of Chinese national leadership. Hungary's deviation from the collective efforts of European Union to divest and decouple from Chinese telecommunications infrastructure has put it in a position in which it experiences friendlier relations with Beijing more than the rest of the continent,[80] but also distances itself from the EU's political leadership as a result of such relations to the point of being characterized as a "Trojan horse."[81] The second danger is the danger to Hungary itself from clans and organizations within the rather than China's overall political leadership. With this dimension, the potential exists for hostile action being committed on the part of Chinese elements without the knowledge and consent of national leadership. Such actions are more likely to be oriented towards Chinese affairs in Hungary rather than wider geopolitical affairs. The potential of cyber-based hostilities directly aimed against

Hungary is much more possible in this scenario given the nebulous nature of identifying the perpetrator of AI-based action and what actors would be more likely to have such motivations. Each issue requires differing responses from Hungary. The options for Hungary to avoid these dangers employ the tactics of "de-risking" and diversification in investments.

With regards to the challenges towards Hungary's relations with the European Union and the U.S., de-risking offers an option that alleviates the security concerns of the U.S. and the European while maintaining economic relations with China. De-risking would involve ensuring proper security precautions were observed for critical infrastructure necessary for ensuring both national and regional collective security while projects that focus on economic development would remain intact. This approach would offer an avenue to maintain economic relations as opposed to outright decoupling. As explained by the Center for Strategic and International Studies (CSIS), "Decoupling entails a complete economic disentanglement," whereas "de-risking is based on the recognition of a threat."[82] In the case of Hungary, "the threat" is the establishment of critical infrastructure such as telecommunications.

An example of this situation in the case of Hungary is the development of the nation's emergency management communications system detailed earlier. De-risking such a system would most likely prove to be untenable without significant capital if not an outright all-new project. Such a situation exists with much of China's investments into Hungary's cyber infrastructure and research and development of artificial intelligence. With a situation as delicate as this, close consultation between Budapest and its collective security partners would be required to determine what points of infrastructure critical to their joint defense may be compromised or vulnerable. A possible solution to such a problem has been previously proposed. The German Council of Foreign Relations identifies three key areas in which Germany has exposure to risks from China due to heavy investment: macroeconomics, security, and political economy,[83] similar to Hungary's current status. While it seeks to address the concerns regarding security vulnerabilities, Germany acknowledges that it does seek to continue its economic relations with China in light of the prosperity brought by the relationship. The key policy recommendations the report makes are to work in concert with the rest of Europe through a proposed "European Economic Security Council" for identifying security risks and proposing collective action and to limit Chinese investment with a more diverse portfolio.[78] The pursuit of such a strategy would strengthen Hungary's strained relations with Europe and the U.S. while maintaining its economic relations with China.

The danger of hostile action by specific clans or individual organizations within the Chinese Communist Party meanwhile can be negated or diluted through diversification of investment. While establishing culpability behind hostile A.I.-based action against Hungarian cyber-augmented infrastructure would be untenable, a more deterrent-based approach would have a much stronger likelihood of avoiding such a danger altogether. The key advantage to Hungary in this situation is its standing as China's most cordial relationship. While Hungary would be able to court other investors, Chinese businesses will be hard-pressed to find an atmosphere as welcoming as Hungary in another European state with regards to the current level of the continent's wariness towards China. Should Chinese businesses overreach in their efforts at influencing Hungarian policies through coercive action, alternatives would both offer Hungary an opportunity to limit and compensate the fallout as well as act as a deterrent to hostile actors by demonstrating they're lack of leverage. Again, Germany has also experienced a similar situation, with the German Foreign Relations Council acknowledging investment diversity as a strategy to address the issues of macroeconomics and political economy.[84]

What these options provide are the ability for Hungary to maintain its relations with Europe and the U.S. while continuing economic relations with Hungary. While the full capabilities of hostile A.I. are not fully understood at the time of this report, their consequences on Hungary's security relationships are evident. The recent advent of this technology, and its constant evolution, make its nature and potential difficult to fully comprehend. This unknown nature, along with the current lack of a collective effort or vehicle in Europe, is what has led to the increased tensions between Hungary and its European and American partners over its relations with China. Steps taken to address such concerns through collective efforts at standard security policymaking while ensuring that economic interests are acknowledged and maintained offer Hungary the strongest position to maintain its relations with all parties.

Author Bios

Logan West is a Research Fellow at the Danube Institute focusing primarily on geopolitical cyber affairs and was the project leader for this product.

Matthew McCracken is policy analyst and researcher currently pursuing a Master of Arts in Public Policy at Liberty University's School of Government.

Eric Hendricks is a Visiting Fellow at the Danube Institute and focuses on Chinese political thought and affairs.

Wael Taji is a doctoral candidate at Semmelweis Unversity and researches the impact of artificial intelligence on society.

Endnotes

[1] Logan West is the primary author of this section.

[2] https://www.nato.int/docu/review/articles/2020/09/30/nato-and-the-5g-challenge/index.html

[3] https://hungarytoday.hu/the-geopolitical-relevance-of-viktor-orbans-planned-trip-to-china/

[4]https://www.cnbc.com/2023/06/27/china-decoupling-would-be-suicide-for-europe-hungarys-pter-szijjrt.html

[5] Matthew MacCracken is the primary author of this section.

[6]https://www.forbes.com/sites/wadeshepard/2017/02/25/another-silk-road-fiasco-chinas-belgrade-to-budapest-high-speed-rail-line-is-probed-by-brussels/?sh=707a80993c00.

[7]Chengfan Zhao, "China and Hungary join forces to develop a new logistics center," Railfreight.com, 21 April 2023, https://www.railfreight.com/beltandroad/2023/04/21/china-and-hungary-join-forces-to-develop-a-new-logistics-center/?gdpr=deny.

[8]"The Intermodal Gate of East and West," East-West Gate Intermodal Terminal Hungary, https://eastwestil.com/en/.

[9]Ganyi Zhang, "Hungary, a promising logistics hub for China-Europe connection," Upply, 22 June 2021, https://market-insights.upply.com/en/hungary-a-promising-logistics-hub-for-the-china-europe-connection.

[10] "Central European Logistics and Industrial Zone," CECZ, https://cecz.eu/en/industrial-park.

[11] "War created an interesting situation in a settlement in northeastern of Hungary," CELIZ, https://celiz.org/war-created-an-interesting-situation-in-a-settlement-in-northeastern-of-hungary/?lang=en.

[12] Zhang, "Hungary, a promising logistics hub for China-Europe connection."

[13] Pablo Gorondi, "Hungary says Huawei to help build its 5G wireless network," Associated Press, https://apnews.com/article/688e48fac84a4eeca73fdb5e17732c5f.

[14] Vlad Makszimov, "Hungary's emergency infrastructure hardware built by Huawei," Euractiv, 20 November 2019, https://www.euractiv.com/section/5g/news/hungarys-emergency-infrastructure-hardware-built-by-huawei/.

[15] Ádám Bráder, "Hungary at the Forefront of Digitalisation," The Hungarian Conservative, May 15, 2023, https://www.hungarianconservative.com/articles/current/digitalisation_hungary_huawei_china_agreement_nke_scholarship/.

[16] "The world's first smart 5G railyard," Huawei, https://www.huawei.com/ie/media-center/our-value/the-world-first-smart-rail-logistics-terminal.

[17] "Huawei takes leap into future with Hungarian supply center," Xinhua, http://english.news.cn/europe/20220308/949b6fa54d4d4c249898e9328f58e13b/c.html.

[18] Karen Gilchrist, "China Decoupling would be 'Suicide' for Europe, Hungary's Foreign Minister says," CNBC, June 27, 2023, https://www.cnbc.com/2023/06/27/china-decoupling-would-be-suicide-for-europe-hungarys-pter-szijjrt.html.

[19] Tamas Csonka, "Hungary says another Chinese battery investment is coming," Intellinews, 12 June 2023, https://www.intellinews.com/hungary-says-another-chinese-battery-investment-is-coming-281374/.

[20] "Chinese BYD May Set Up its First European Car Plant in Hungary," Hungary Today, https://hungarytoday.hu/chinese-byd-may-set-up-its-first-european-car-plant-in-hungary/

[21] Gilchrist, "China Decoupling would be 'Suicide' for Europe, Hungary's Foreign Minister says."

[22] "Hungary – EU Member Country Profile," European Union, https://european-union.europa.eu/principles-countries-history/country-profiles/hungary_en.

[23] Eric Hendricks was the primary author of this section.

[24] https://global.chinadaily.com.cn/a/202302/21/WS63f400dca31057c47ebafd3b.html

[25] Ursula von der Leyen, "Speech by President von der Leyen on EU-China relations to the Mercator Institute for China Studies and the European Policy Centre," 30 Mar. 2023. https://ec.europa.eu/commission/presscorner/detail/en/speech_23_2063

[26] Thomas W. Pauken II, "Why Does Hungary Take the Lead in Promoting China-Europe Connectivity?", China Focus, 31 Oct. 2023, http://www.cnfocus.com/why-does-hungary-take-the-lead-in-promoting-chinaeurope/.

[27] Mária Schmidt, "China Has Made an Alliance With Time," About Hungary, 29 Oct. 2023, https://abouthungary.hu/blog/china-has-made-an-alliance-with-time.

[28] Laura Silver, Christina Huang, and Laura Clancy, "Views of China," Pew Research Center website, 27 Jul. 2023, https://www.pewresearch.org/global/2023/07/27/views-of-china/#:~:text=Attitudes%20toward%20China%20are%20largely,just%2028%25%20offer%20positive%20ratings

[29] Matura, "Hungary," 78.

[30] World Economic Outlook Database, April 2023.

[31] World Intellectual Property Organization (WIPO), Global Innovation Index 2022: What is the Future of Innovation Driven Growth?, 15th edition, ed. Soumitra Dutta, Bruno Lanvin, Lorena Rivera León, and Sacha Wunsch-Vincent (Geneva: WIPO, 2022), 19, doi: 10.34667/tind.46596.

[32] "Most Influential Countries," U.S. News, https://www.usnews.com/news/best-countries/most-influential-countries

[33] Grzegorz Stec, "'Correct Choice' on Strategic Autonomy: What China Wants from the EU," MERICS Briefs, 28 Apr. 2021, https://merics.org/en/merics-briefs/correct-choice-strategic-autonomy-what-china-wants-eu.

[34] Ibid.

[35] Jorge Liboreiro, "China's Divide-and-Conquer Tactics Are Already 'in Action,' Ursula von der Leyen Warns," Euro News, 18 Apr. 2023, https://www.euronews.com/my-europe/2023/04/18/chinas-divide-and-conquer-tactics-are-already-in-action-ursula-von-der-leyen-warns

[36] Grzegorz Stec, "'Correct Choice'."

[37] Cao Chuanchuan (曹川川), "Xi Calls with German Chancellor Angela Merkel" (习近平同德国总理默克尔通电话, Xíjìnpíng tóng déguó zǒnglǐ Mòkèěr tōng diànhuà), Xinhua, Xinhua, 8 Apr. 2021, http://xitheory.china.com.cn/2021-04/08/content_77386839.html.

[38] Demetri Sevastopulo, Henry Foy, John Paul Rathbone, and Joe Leahy, "Chinese Spies Recruited European Politician in Operation to Divide West," Financial Times, 15 Dec. 2023, https://www.ft.com/content/601df41f-8393-46ad-9f74-fe64f8ea1a3f.

[39] Marc Hijink, "Resigned ASML Employee Went to Huawei—and Took Trade Secrets with Him" (Opgestapte ASML-medewerker ging naar Huawei – en nam bedrijfsgeheimen mee), NRC, 23 Oct. 2023, https://www.nrc.nl/nieuws/2023/10/23/oud-asmler-nam-bedrijfsgeheimen-mee-naar-huawei-a4178222.

[40] Jordan Robertson and Michael Riley, "Engineer Who Fled Charges of Stealing Chip Secrets Now Thrives in China (Repeat)," Bloomberg, 15 Feb. 2023, https://www.bloomberg.com/news/articles/2022-06-06/engineer-who-fled-us-charges-of-stealing-chip-technology-now-thrives-in-china.

[41] Sevastopulo, Foy, Rathbone, and Leahy, "Chinese Spies Recruited European Politician," Financial Times.

[42] Ibid.

[43] Pierre Bourdieu, "Appendix: The 'Soviet' Variant and Political Capital," in: Pierre Bourdieu, Practical Reason: On the Theory of Action, trans. from French by Randal Johnson and others (Stanford, CA: Stanford University Press, 1998), 14–18.

[44] Eric Hendriks-Kim, "The Polemics of China's Counter Cosmopolitanism," Telos 201 (Winter 2022), 13–37; here 26–30.

[45] Richard McGregor, The Party: The Secret World of China's Communist Rulers (New York: HarperCollins, 2010), 3.

[46] Pau J. DiMaggio, Walter W. Powell, "The Iron Cage Revisited: Institutional Isomorphism and Collective Rationality in Organizational Fields," in: American Sociological Review (1983) 48.2, 147–160, doi:10.2307/2095101

[47] Yanjie BIAN, “Guanxi Capital and Social Eating in Chinese Cities: Theoretical Models and Empirical Analyses,” in Social Capital: Theory and Research, ed. Nan Lin, Karen Cook, Ronald S. Burt (New York: Aldine De Gruyter, 2001), pp. 275–296.

[48] Ibid.

[49] Ibid.

[50] Guo Xuezhi, “Dimensions of Guanxi in Chinese Elite Politics,” The China Journal (Jul. 2001) 46, doi: 10.2307/3182308

[51] McGregor, The Party, 170–193.

[52] Ibid.

[53] Compare: Interview with Edward Luttwak by David Dusenbury and Eric Hendriks, “The Autism of Great Powers,” Buda Hills podcast, 1 Aug. 2023, https://www.youtube.com/watch?v=aCmV6_jXLgo.

[54] Robert E. Kelly, “What are the Chinese Telling Us by Bullying South Korea so Much over Missile Defense?”, Robert E Kelly, 29 Jan. 2017, https://robertedwinkelly.com/2017/01/29/what-are-the-chinese-telling-us-by-bullying-south-korea-so-much-over-missile-defense/.

[55] Ibid.

[56] The following passage from Phoebe Moon’s interview with Legislator Kim details the conversation: “A researcher at the Chinese Academy of Social Sciences (中国社会科学院) called me back in 2017 and asked what Seoul’s stance was on the China-South Korea relations. I expressed great discomfort. […] I told him that when Presidential Candidate Moon gets elected he has no choice but to strengthen our alliance with the US rather than pursuing balanced diplomacy, if China keeps on fomenting anti-China sentiment among South Koreans like this. He was dumbstruck [my italics] by my comment. […] I met a lot of high-ranked CCP diplomats including Yang Jiechi (杨洁篪) and Xing Haiming (邢海明). Whereas China pressured South Korea to be balanced between China and the US in the past, Beijing now respects the US-South Korea alliance much more and is worried about it.”” Phoebe Moon, When the Target Fights Back: Economic Coercion and Interstate Conflict in the Era of Global Value Chains (UC Irvine Electronic Theses and Dissertations, 2022), 160, https://escholarship.org/uc/item/240950rx.

[57] Wael Taji was the primary author of this section.

[58] “Pegasus: What you need to know about Israeli spyware,” Al Jazeera, 8 Feb 2022, https://www.aljazeera.com/news/2022/2/8/what-you-need-to-know-about-israeli-spyware-pegasus

[59] Kali Robinson, “How Israel’s Pegasus Spyware Stoked the Surveillance Debate,” Council on Foreign Relations, March 8 2022, https://www.cfr.org/in-brief/how-israels-pegasus-spyware-stoked-surveillance-debate

[60] Ronen Bergman and Mark Mazzetti, “The Battle for the World’s Most Powerful Cyberweapon,” New York Times, Jan 28 2022, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html

[61] Aina Marzia, “Automated Apartheid: How Israel’s Occupation is powered by big tech, AI, and spyware, The New Arab, July 03 2023, https://www.newarab.com/analysis/how-ai-big-tech-and-spyware-power-israels-occupation

[62] Madyson Fitzgerald, “What is artificial intelligence? Legislators are still looking for a definition.” Stateline, October 5 2023, https://stateline.org/2023/10/05/what-is-artificial-intelligence-legislators-are-still-looking-for-a-definition/

[63] Dewey Murdick, James Dunham and Jennifer Melot, "AI Definitions Affect Policymaking," Center for Security and Emerging Technology, Georgetown University, June 2020, https://cset.georgetown.edu/publication/ai-definitions-affect-policymaking/

[64] Reza Montasari (2023), "Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK Cybersecurity", Springer, p82

[65] Stephen Ornes, "The Unpredictable Abilities Emerging from Large AI Models," Quanta Magazine, March 16 2023, https://www.quantamagazine.org/the-unpredictable-abilities-emerging-from-large-ai-models-20230316/

[66] Ibid

[67] An obvious and tangible example of AIPs in the real world can be found in ChatGPT - a Large Language Model (LLM) developed by OpenAI. In a literal sense, the act of posing a question to ChatGPT is no different to putting code into the command line of a Python script; in such instances, the human user provides the machine with an input, and in doing so, instructs it to respond by generating a corresponding output. Where ChatGPT (and AI more broadly) diverge is in the response (procedurally and materially). Inputting correct code into a Python script can only lead to two possible outcomes: either the script will work, or the script won't work. In stark contrast to this predictable and simple process structure, a prompt given to an AI-augmented process such as ChatGPT results in an output that cannot be predicted, even by the engineers responsible for programming the process itself. This feature, where the same input can produce different and entirely unpredictable outputs, is the core and most consequential feature of AI systems, including those used in the context of cyber warfare.

[68] "Kuldeep Tomar & Shivani Sharma (2023). "A proposed artificial intelligence and blockchain technique for solving health insurance challenges". In "Data-Driven Technologies and Artificial Intelligence in Supply Chain: Tools and Techniques". Edited by Manesh Chand, Vineet Jain, & Puneeta Ajmera. CRC Press, p38.

[69] Patrick Thibodeau, "How Trump, Biden see automation and AI," TechTarget, Sep 29 2020, https://www.techtarget.com/searchhrsoftware/news/252489763/How-Trump-Biden-see-automation-and-AI

[70] Andrew Yang, "Andrew Yang: Yes, Robots Are Stealing Your Job," New York Times, Nov 14 2019, https://www.nytimes.com/2019/11/14/opinion/andrew-yang-jobs.html

[71] "AI-based production further expands in Bridgestone's unit in Tatabánya – VIDEO REPORT," HIPA, Sep 03 2019, https://hipa.hu/news/artificial-intelligence-based-production-further-expands-in-bridgestone-s-unit-in-tatabanya/

[72] Botond Kálmán and Arnold Tóth, "The Success of Japanese Foreign Market Investments in Hungary," International Journal of Trade, Economics and Finance (August 2021) Vol. 12 No. 4, http://www.ijtef.com/vol12/700-DM1005.pdf

[73] Ibid

[74] Deep Dave and Pranav Wadhera, "How can smart manufacturing prevent industrial espionage and sabotage?" LinkedIn, https://www.linkedin.com/advice/0/how-can-smart-manufacturing-prevent-industrial

[75] "Industrial & Corporate Espionage: What Is It, Cases & Best Prevention Practices," Ekran, March 24 2023, https://www.ekransystem.com/en/blog/prevent-industrial-espionage

[76] Adi Gaskell, "Is gut instinct as effective as AI at spotting fakes online?" cybernews, Nov 15 2023, https://cybernews.com/security/is-gut-instinct-as-effective-as-ai-at-spotting-fakes-online/

[77] "Defense.gov News Transcript: DoD News Briefing – Secretary Rumsfeld and Gen. Myers". United States Department of Defense. February 12, 2002. Archived from the original on April 6, 2016

[78] Logan West was the primary author of this section.

[79] "China's Xi says he considers Hungary's Orban a 'friend'," Reuters, Oct 17 2023, https://www.reuters.com/world/chinas-xi-says-he-considers-hungarys-orban-friend-2023-10-17/

[80] François Venne, "China's Trojan Horse Canters Through Hungary," CEPA, April 19 2021, https://cepa.org/article/chinas-trojan-horse-canters-through-hungary/

[81] Lily McElwee, "Beijing's Emerging Assessment of De-risking," CSIS, Oct 17 2023, https://www.csis.org/analysis/beijings-emerging-assessment-de-risking

[82] Ole Spillner and Guntram Wolff, "China "De-risking" A Long Way from Political Statements to Corporate Action," DGAP, German Council on Foreign Relations, June 2023, https://dgap.org/system/files/article_pdfs/dgap-policy brief-2023-15-en-AG Zeitenwende-GW.pdf

[83] Ibid

[84] Ibid

Bibliography

Andrea Gilli, Francesco Bechis. "NATO and the 5G Challenge," NATO Review, 30.09.2020.

Dewey Murdick, James Dunham, and Jennifer Melot. "AI Decisions Affect Policymaking," CSET Analysis, 02.06.2022.

European Union. "Hungary," EU Member Country Profiles, accessed 15.08.2023

François Venne. "China's Trojan Horse Canters though Hungary," CEPA Insights and Analysis, 19.04.2021.

Ganyi Zhang. "Hungary, a Promising Logistics Hub for the China-Europe Connection," Upply Market Insights, 22.06.2021.

German Council on Foreign Relations. "China "De-risking" A Long Way from Political Statements to Corporate Action," DGAP Policy Brief No. 16, June 2023.

Grzegorz Stec, "'Correct Choice' on Strategic Autonomy: What China Wants from the EU," MERICS Briefs, 28.04.2021.

Phoebe Moon. "When the Target Fights Back: Economic Coercion and Interstate Conflict in the Era of Global Value Chains," UC Irvine Electronic Theses and Dissertations, 2022, 160.

Reza Montasari (2023), "Countering Cyberterrorism: The Confluence of Artificial Intelligence, Cyber Forensics and Digital Policing in US and UK Cybersecurity", Springer, 82.

Richard McGregor, The Party: The Secret World of China's Communist Rulers (New York: HarperCollins, 2010).

Stephen Ornes. "The Unpredictable Abilities Emerging From Large AI Models," Quanta Magazine, 16.03.2023.

Vlad Makszimov. "Hungary's emergency infrastructure hardware built by Huawei," Euractiv, 08.11.2019 (updated 20.11.2019).

Yanjie Bian. "Guanxi Capital and Social Eating in Chinese Cities: Theoretical Models and Emirical Analysis," Social Capital: Theory and Research, ed. Nan Lin, Karen Cook, Ronald S. Burt, Ney Work: Aldine De Gruyter, 2001.