FIIA
BRIEFING PAPER

JUNE 2019 /267

GEOSTRATEGICALLY MOTIVATED CO-OPTION OF SOCIAL MEDIA

THE CASE OF CHINESE LINKEDIN SPY RECRUITMENT

Mika Aaltola

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

GEOSTRATEGICALLY MOTIVATED CO-OPTION OF SOCIAL MEDIA

THE CASE OF CHINESE LINKEDIN SPY RECRUITMENT

- Social media platforms enable a strategically motivated and harmful set of practices that leverage both their scalability and targeting potentials.
- The wider vulnerabilities of digitalized democracies have been much discussed in connection with election meddling and disinformation campaigning. However, the emphasis here is on the more direct vulnerability of mass spy recruitment.
- The ongoing LinkedIn-based mass recruitment provides a case in point, representing a dangerous vulnerability that can lead to the theft of intellectual property and confidential materials, as well as to the setting up of influence networks.
- This Briefing Paper details the Chinese co-option of LinkedIn for gaining operatives in and confidential information from Western states and enterprises.
- Exposing the emerging adversary techniques used by resourceful state actors is the first counter-step. Moreover, preparedness needs to be highlighted, counter-measures modernized, and laws updated to address the new vulnerabilities.

MIKA AALTOLA

Programme Director

Finnish Institute of International Affairs

ISBN 978-951-769-611-1
ISSN 1795-8059
Language editing: Lynn Nikkanen.
Cover photo: Pixabay.
Used under the Creative Commons license.

FIIA
FINNISH
INSTITUTE
OF INTERNATIONAL
AFFAIRS

Arkadiankatu 23 b
POB 425 / 00101 Helsinki
Telephone +358 (0)9 432 7000
Fax +358 (0)9 432 7799

www.fiia.fi

The Finnish Institute of International Affairs is an independent research institute that produces high-level research to support political decisionmaking and public debate both nationally and internationally.
All manuscripts are reviewed by at least two other experts in the field to ensure the high quality of the publications. In addition, publications undergo professional language checking and editing. The responsibility for the views expressed ultimately rests with the authors.

GEOSTRATEGICALLY MOTIVATED CO-OPTION OF SOCIAL MEDIA

THE CASE OF CHINESE LINKEDIN SPY RECRUITMENT

INTRODUCTION

The emergence of a more competitive power-political situation shifts rivalry into the economic and technological fields, as the costs of an open and direct military conflict remain very high in the nuclear age. The key strength of Western democracies is commonly attributed to their open economies and highly digitalized societies. However, these characteristics can also turn into vulnerabilities. The practices of geostrategic competition are evolving and can co-opt the ongoing information technological revolution. Many of the highly digitalized Western states have been waking up to the new types of power-political competition occurring in the social media domain. At the same time, the Western states have also developed capabilities as showcased by the 'Snowden revelations'. Yet efforts have largely been channelled into the fight against terror, not geopolitical rivalry.

It can be argued that geopolitical practice is increasingly changing from direct and indirect territorial competition over strategic resources into competition over direct or indirect control of the key functions of global connections, such as the maritime, air, space, and digital domains. The focus here is on the newer type of functional competition over the digital domain and its social media platforms.

For resourceful state-level players, these new vulnerabilities offer lucrative, exploitable opportunities by: (1) Destabilizing: innovating new means of sowing and catalyzing societal divisions before, during and after democratic processes such as elections and referendums. (2) Scaling up: massively scaling up older practices such as espionage, as well as building multi-purpose informer, influence, and corruptive networks.

In the first sense, social media can be utilized as a part of destabilizing campaigns, as the recent redacted version of the 2019 Mueller Report – presenting the findings of the official investigation into Russian meddling in the 2016 US elections – revealed. One aspect of the meddling operation was the use of the Russian quasi-governmental Internet Research Agency (IRA) across different social media platforms. According to the report, 'by the end of the 2016 U.S. election, the IRA had the ability to reach millions of U.S. persons through their social media accounts. Multiple IRA-controlled Facebook groups and Instagram accounts had hundreds of thousands of U.S. participants. IRA-controlled Twitter accounts separately had tens of thousands of followers, including multiple U.S. political figures, who retweeted IRA-created content'.[1] The digitalized geopolitical abuses of the platforms were also in evidence in European politics. Most of the discussions in this respect have focused on the 2017 French and German elections, and on the 2016 UK referendum on EU membership.

Moreover, the growing role of digitalized platforms offers less well-known opportunities for scaling up old power-political practices. The focus here is on a lesser-known but emerging vulnerability, the hybrid use of social media platforms to catalyze espionage and the establishment of influence networks. This is evidenced by the strategic abuse of one of the more career-oriented digital platforms, LinkedIn. Whereas on Facebook and Twitter the content is more about news and political debates and on Instagram mostly about images, the political nature of LinkedIn is different. LinkedIn is based on posting information on professional status, finding work and business opportunities, navigating professional life, networking, and establishing a professional community.

The use of the LinkedIn platform for mass spy recruitment by the Chinese authorities is an alarming case in point when it comes to the changing landscape of major power competition in the digital age. The scramble to keep highly digitalized societies secure against new illicit influence operations requires a more serious effort. However, the nexus between new geopolitical rivalry and emerging technologies is a tricky issue. The continuing evolution of the competitive practices remains a mystery in itself, with the increased likelihood of further detrimental operations and campaigns. Hence, the implications of this study

[1] Special Council Robert Mueller (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election. U.S. Department of Justice.

extend beyond mass espionage operations. For example, it is possible that the mass recruitment operations support dark money networks and empower politically motivated corruptive operations.

POWER-POLITICAL VULNERABILITIES OF THE DIGITALIZED PUBLIC SPHERE

As domestic networking and debates increasingly take place on algorithmic digitalized social media platforms, the materiality and political effects of the technology have become topical issues. There are different established ways to disrupt, abuse, and leverage digitalized platforms. These qualities are inherent in and endogenous to the underlying technology and practices of the user (e.g. individuals, enterprises, and states):

1. Ease of scalability: The platforms offer ways of directly reaching very large audiences with relatively little cost or difficulty.
2. Smart targeting: Finding the 'needle in the haystack' used to require more labour. Now, with the help of innovative AI-based algorithmic tools, it is possible to use the available big data to find the 'right' users, and to tailor content that appeals to them.

These characteristics also offer new opportunities for older intelligence practices and lead to innovative practices that were laborious or impossible before. Finding informants and spies used to be a long and meticulous process. Thanks to social media platforms, spotting and recruiting people has become significantly easier. At the same time, mass surveillance for social and political control inside and outside of the country is now becoming more widespread, especially in technologically advanced autocracies such as China.

There are several reasons why the Microsoft-owned LinkedIn is particularly attractive to a capable state actor for a mass recruitment effort. Besides students, recent graduates and job-seekers, LinkedIn is used and frequented by decision-makers and executives. According to LinkedIn's own statistics, the platform's membership includes 61 million senior-level influencers and 40 million decision-makers.[2] It is geared towards showcasing one's professional experience and expertise. Users are looking for content and opportunities that can change the way they do business or shape the direction of their careers. Overall, the platform has 500 million members, 260 million of whom log in monthly, with about 40 per cent of the monthly users logging in every day.

Furthermore, LinkedIn is geographically widespread. The platform has agreed to adhere to China's legal and governmental requirements and has been able to operate in the country as a result, currently hosting approximately 41 million Chinese users.

Besides enabling analysis of user-posted data, LinkedIn allows for a broad recruitment operation resembling a fishing expedition, where the 'net' is cast relatively wide, and deniability is possible because the true identity of the recruiters is difficult to attribute through the use of fake accounts as a front for the operation.

THE PUBLICLY REPORTED LINKEDIN MASS RECRUITMENT CASES

The German domestic intelligence agency (BfV) revealed in late 2017 that China had used fake LinkedIn accounts to gain access to confidential information on German officials and politicians. The number of individuals that had been approached amounted to more than 10,000. According to the agency, this was 'a broad-based attempt to infiltrate in particular parliament, ministries and government agencies'.[3] In order to counteract the hostile operation, the BfV published details of eight fake accounts.

In August 2018, the US publicly accused China's intelligence agencies of using LinkedIn in a campaign to recruit Americans. According to US counterintelligence information, the recruitment effort was unusually broad, with at least thousands being targeted. The recruitment campaign targeted people who were likely to have access to confidential and secret commercial or governmental information.

Aside from the aforementioned publicly revealed incidents, there have been reports of Chinese mass operations in other Western countries. For example, the French media reported on a leaked French intelligence report detailing that 4,000 individuals had been approached by Chinese fake LinkedIn accounts.

[2] LinkedIn (16.11.2016). Get Proof: The Case for B2B Marketing on LinkedIn. https://business.linkedin.com/marketing-solutions/blog/linkedin-b2b-marketing/2016/get-proof--the-case-for-b2b-marketing-on-linkedin--infographic-.

[3] AP (10.12.2017). German intelligence warns of increased Chinese cyberspying. https://www.apnews.com/5f15f9c016f547e4812ba6b2ee66b896.

Among the targets were civil servants and company executives. [4]

LinkedIn is populated by people seeking new opportunities. It is possible to find – by careful analysis of posted information – individuals whose careers have floundered and who are possibly experiencing financial troubles. If a person's list of prior experience includes sensitive and confidential positions, such as former member of parliament or military or intelligence posts, there is a clear incentive to try to lure them into a trap.

For example, Kevin Mallory, a former CIA officer, was sentenced to 20 years in prison for handing over secret documents and confidential information to Chinese intelligence. His career was floundering and he was in dire financial straits when he received a message from a fake account on LinkedIn in 2017. This fake contact claimed to be working for a think tank that was looking for foreign policy expertise. The targeted ex-CIA officer travelled to China twice and was given money and equipment to maintain his communications with the Chinese.[5]

THE RECRUITMENT LADDER

The following steps are based on the publicly available information on the German, US and French cases as well as on confidential cases in Finland, where at least several foreign policy experts were approached via LinkedIn messages.[6] The targeted Finnish individuals were academics with knowledge of Finnish foreign and security policy. The following analysis of recruitment steps is also based on reviewed LinkedIn messages and other messages sent to the targets.

Target spotting and defining the target range can be done algorithmically: identifying a possible target for recruitment used to be a delicate process, carried out by trusted assets with deep covers in the target state's organizations or by experienced intelligence officers. They painstakingly compiled the target lists and established patterns in order to approach the identified targets.

However, with the data made available by LinkedIn, it is possible to approach a relatively large number of people working in a chosen field and possessing promising expertise or skills. This can be done in conjunction with the old practices. Locally knowledgeable targeters can subsequently be used later on in the process to evaluate the quality of those targets caught in the net of the automated LinkedIn method.[7] One obvious problem is that the mass recruitment is likely to be picked up by the target state's intelligence services. This means that promising targets could actually be working for the target state's intelligence. This danger needs to be mitigated by careful screening of targets, for example by testing their data and finding out more about them through the available metadata, such as credit histories, medical data and other information that is helpful in profiling.

Through metadata analysis and human intelligence, it becomes possible to narrow down the range of targets to a desired subset. Having a fairly large number of targets increases the likelihood of inducing at least a few to proceed deeper into the recruitment net.

The first approach is made by using fake social media profiles: After the evaluation of the possible informants, the LinkedIn operation approaches the targets with promises of easy money and expressions of appreciation for their expertise. The targets are approached by fake profiles, which are made to seem credible with stylish photos, professional information and references to reputable organizations. Even AI-generated faces can be used.[8] The fake profiles appear to be dynamic professionals, consultants, headhunters or think-tankers. In the publicized German case, the fake profile 'Laeticia Chen' was supposed to be a successful manager at the China Center of International Politics and Economy. The centre itself had a web presence and could be googled by the interested targets, as is common practice nowadays for people looking for new opportunities.

The fake account approaches the targets with a stock message asking for a short report on a wide range of topics, some of which would clearly fall within the range of the target person's expertise. The message is likely to attract attention because of the promise of a fair amount of money compared to the seeming ease of the required job. Even if the thought occurs to the

[4] For example, Bloomberg (23.10.2018). French Are Target of Widespread Spying by Chinese, Figaro Says, https://www.bloomberg.com/news/articles/2018-10-23/french-are-target-of-widespread-spying-by-chinese-figaro-says.

[5] For example, NBC News (9.4.2019). How a $230,000 debt and a LinkedIn message led an ex-CIA officer to spy for China, https://www.nbcnews.com/politics/national-security/how-230-000-debt-linkedin-message-led-ex-cia-officer-n990691.

[6] These cases of approached foreign policy experts cannot be disclosed in detail due to their confidential and sensitive nature. This Briefing Paper draws on interviews with those who were targeted.

[7] Wired (11.10.2018). How the US forced China to quit stealing – using a Chinese spy, https://www.wired.com/story/us-china-cybertheft-su-bin/.

[8] AP (13.6.2019). Experts: Spy used AI-generated face to connect with targets, https://apnews.com/bc2f19097a4c4fffaa00de6770b8a60d.

target that there is something shady about the proposal, the activity itself – writing a short report – is not illegal in many Western countries if no secret or confidential information is revealed.

It should be noted that this money-based approach seems to be at odds with the Cold War era's best practice and lessons learnt. It was previously thought that money should not be the primary motive in recruitment.[9] It seems that in the LinkedIn operation, these risks are considered low from the recruiter's perspective, or can be mitigated in later phases. It should also be noted that the Chinese mass recruitment method contains an element of 'ego'. The cultivated targets are made to feel unique, as their expertise is noticed and considered valuable.

It is also possible that the situation has changed considerably from the Cold War years, as ideological contestation has receded into the background. Ideological competition does not provide as effective a vector for recruitment as it used to. At the same time, the Western awareness of Chinese money has been based on seeing opportunities rather than shady risks. Much effort is exerted in making the process seem like a normal business proposal. The risks of becoming a participant in politically underhand activities have been more associated with Russian money than with Chinese, although Chinese theft of intellectual property has been making headlines for years.

The target is introduced to the next steps of the 'ladder': The target is told about the possibility of earning more money if they produce more detailed written material. Soon after the initial report, more instructions are given for writing the report and the chosen topics. Before long, it is stated that the material submitted is not supposed to be based on 'publicly available sources' or on 'information found via Google'.

If the target is working in a confidential position and has access to confidential material, it is suggested that providing information of this type will lead to further financial gain. Next, special emphasis is put on the target producing actual photos of authentic confidential or secret documents.

The next step could be called 'What happens in China, remains in China': Relatively early on in the process, the recruiters tell their targets that an all-expenses-paid trip to China would facilitate the process, and would allow for the secure delivery of an even larger sum of money. It is likely that the final assessment of the target's potential value is made during this trip.

In the final phase, the target becomes hooked: The person is by now fully aware of the illicit nature of the activities. However, the transactions already made can be used for implicit blackmail, although the coercion is more implied than real. During the recruitment process, the emphasis is on giving the impression that the target's security is highly protected by their new Chinese 'friends'. The impression is also given that the financial rewards will grow if the person is willing to take on a more active role, as an influence agent, informant, or a spotter of other targets.

THE WEAKENED WESTERN IMMUNITY

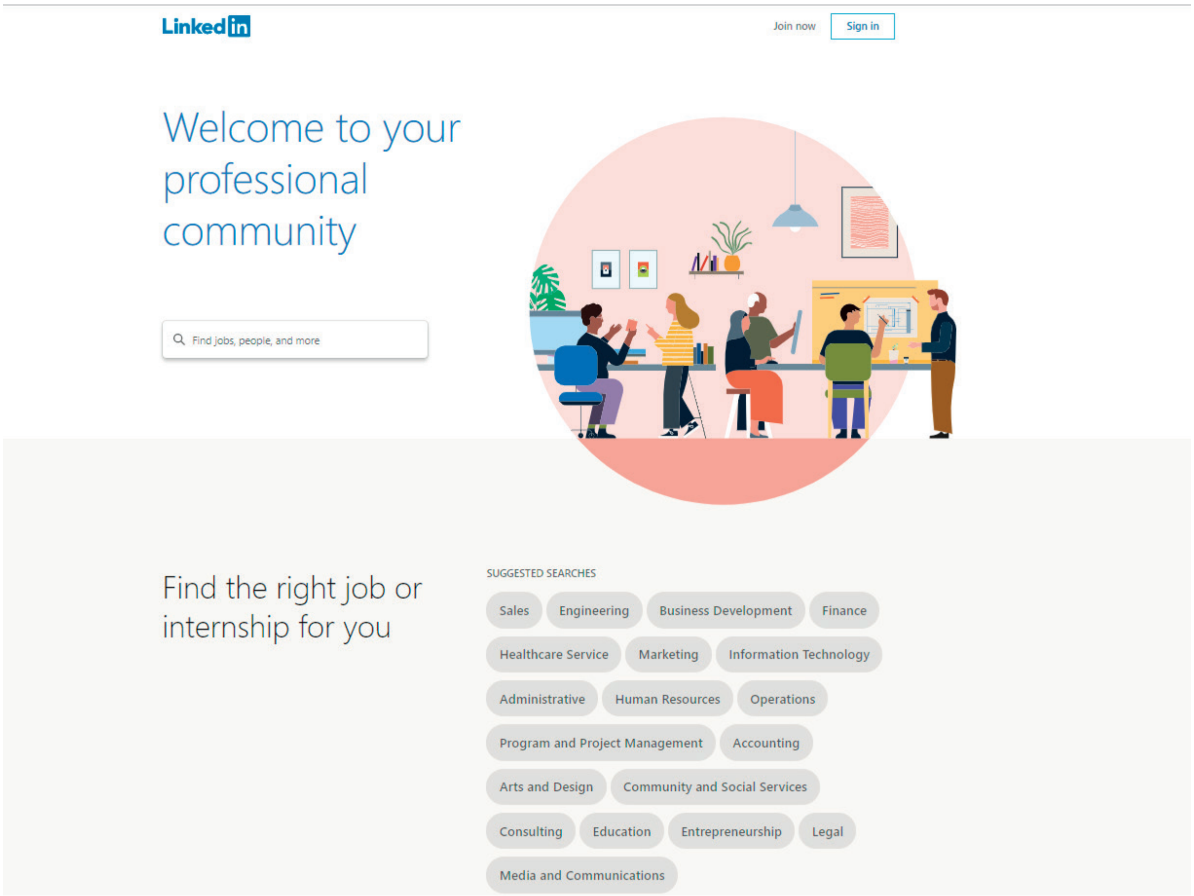
The effectiveness of the mass recruitment through LinkedIn is difficult to evaluate as the scale of the activities largely remains unknown. However, it is clear that it has been successful from the Chinese perspective, as it is still ongoing.

The Western states have experienced changes since the Cold War years. It can be argued that a sense of vigilance, mobilization, and cohesion in the face of geopolitical competition receded into the background in the 1990s. Many Western states experienced the so-called 'peace dividend' phenomenon. In many Western democracies, the will to sustain the preparedness to take on possible geopolitical rivals decreased. Finances were needed in other sectors. For example, national willingness to defend one's own state or close allies has decreased in many states. According to one recent survey, only 25 per cent of respondents in Western Europe said they would be willing to defend their country militarily.[10] Before the direct geopolitical challenge by Russia in Ukraine, the world was seen as developing in a direction in which geopolitical rivalries would not require constant vigilance and costly mobilization. To a degree, the world was seen as liberalizing, normalizing, and democratizing, in ways that did not require large-scale investments in counter-intelligence.

Secondly, part of this lack of awareness could stem from the other much-highlighted priorities that have emerged, such as funds going into anti-terrorism measures. The events of 9/11 changed the focus in the

[9] Money matters more nowadays since the ideological contestation is less distinct. For an opposing viewpoint, see Burkett, Randy (2013). 'An Alternative Framework for Agent Recruitment: From MICE to RASCLS.' *Studies in Intelligence* Vol. 57, No. 1.

[10] Gallup International (2015). WIN/Gallup International's global survey shows three in five willing to fight for their country, http://gallup-international.bg/en/Publications/2015/220-WIN-Gallup-International's-global-survey-shows-three-in-five-willing-to-fight-for-their-cou.



Welcome to your professional community

Find the right job or internship for you

LinkedIn’s membership includes 61 million senior-level influencers and 40 million decision-makers. They are appealing targets for a foreign intelligence, and recruiting people has become significantly easier.

US, and the rise of ISIS and its strikes in Europe have led to increased funding for the intelligence services. Yet the increased resources have not focused on the increased power-political competition and on the illicit activities of the major power in the West.

Third, awareness of the geopolitics of digital vulnerability has been heightened particularly by Russian attempts to meddle in and influence Western democratic processes. However, the innovations developed by geopolitical competitors in the digital domain have caught many by surprise. This indicates that many Western states may not have fully realized the depth and scope of the social media-related vulnerabilities.

State loyalties can also be overwhelmed by internal feuding and distrust in many of the Western states. This may have a bearing on the Chinese mass recruitment operation. Apart from money and ego, ideology still matters. Trust, solidarity, and the loyalty of the targets can be deflected away from the home state like a cohesive actor that needs to be secured along the new digital frontiers as well.

Identity wars, polarization, and the rise of neo-nationalism in some democracies narrows some people’s identity groups, leading them to identify with domestic out-groups and radical factions. In some Western states, cohesion increasingly depends on perceived animosities towards other domestic groups – more so than towards external competitors, the threat from whom feels less tangible, especially if it occurs through social media platforms in ways that are relatively hard to discern.

Moreover, social media platforms like LinkedIn offer a relatively open and transnational vision of one’s life options. The boundary between what is considered internal to a state and what is seen as external can become increasingly fuzzy and people’s careers more nomadic. As a result, loyalties to one’s own state and its security interests can weaken. The chances of earning a livelihood from one’s expertise, irrespective of state boundaries or loyalties, have been highlighted during the more cosmopolitan post-Cold War era. To a degree, the Chinese mass spy recruitment campaign shows how this cosmopolitan style of living can collide with re-emerging geopolitical rivalries.

IMPLICATIONS AND COUNTER-MEASURES

The leveraging of social media platforms for mass recruitment of new assets and informants is tempting for China's intelligence organizations. Compared to states like Russia, China is an actor without historically, politically, culturally, or deep ethnically nurtured ties to some of the target states. It does not have a long history (in modern times) as a top-tier major power. Its influence has yet to penetrate the business, media, and decision-making elites in Europe and North America. Its power is emerging rather than established and enduring.

The LinkedIn recruitment activities break new ground in the methods employed by China's intelligence agencies.[11] Traditionally, recruitment has occurred among ethnic Chinese in the West, such as graduate students or professionals in strategic industries. Now, with the help of social media platforms, recruitment is increasingly focused on non-Chinese Western nationals. Recently, the suspected cases have started to mushroom into dozens of prosecutions in the US.[12]

In response, the German and US authorities have demanded that LinkedIn close the fake accounts used in the recruitment effort. It is important for social media platforms to adopt new, more responsible policies. LinkedIn should approach the matter in the same way that Facebook, Twitter, and Google responded to the disinformation and trolling campaigns initiated by Russian actors during the Western elections, when they implemented changes, new procedures, and tighter self-regulation.

Lack of attention to the phenomenon among some of the Western publics needs to be remedied by awareness-raising campaigns. Possible target individuals, such as academics, decision-makers and company executives need to be made aware of the possible methods through which they may be approached. Revealing the steps through which an operation can be carried out is among the best ways of rendering it ineffective in the future, as people become aware of what might happen. The laws and legal consequences should also be updated, as in many countries the first steps in the recruitment process are currently not illegal.

[11] In the American LinkedIn case, suspicions fell on the Chinese Ministry of State Security (MSS).

[12] Wired (31.10.2018). China's 5 steps for recruiting spies, https://www.wired.com/story/china-spy-recruitment-us/.