Helsinki in the era of hybrid threats

– Hybrid influencing and the city

Helsinki

Helsinki in the era of hybrid threats
– Hybrid influencing and the city
City of Helsinki, publications of the Central Administration 2018:22
ISBN 978-952-331-474-0 (printed publication)
ISBN ISBN 978-952-331-475-7 (e-publication)
ISSN-L 2242-4504
ISSN 2242-4504 (printed publication)
ISSN 2323-8135 (e-publication)
Cover photo: Klss/Shutterstock.com
Layout: Guassi Oy
Printing house: Edita Prima Oy

Contents

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Helsinki

Preface

Events around the world have also made new types of threats a topic of discussion in Finland. Hybrid influencing, hybrid threats and hybrid warfare are familiar terms from the pages of newspapers and analyses by research institutes. However, the lively news coverage often tends to give less attention to the true nature of *hybrid influencing* as well as its link to local administration and everyday life. This report delves into this topic and seeks to shed light on hybrid influencing as a phenomenon from the perspective of Helsinki.

The report is based on a review of literature and public documents concerning the topic, a survey targeted at members of the City Council, and interviews with a broad range of experts. The experts consulted include representatives of the City of Helsinki, the National Bureau of Investigation, the Hospital District of Helsinki and Uusimaa (HUS), the Finnish Border Guard, the National Emergency Supply Agency (incl. the Public Health Pool and Media Pool), Aalto University, Faktabaari, Cultura, the Regional State Administrative Agency of Southern Finland, CGI and KPMG, among others.

Nevertheless, the report only represents the views of its writers. The report was written by Atte Harjanne, Eetu Muilu, Jekaterina Pääkkönen and Hanna Smith.

The report's roots go back to the Hack for Society project implemented in autumn 2017, in which researchers, students and members of the City Council solved challenges faced by Helsinki in close cooperation as a working group. The insights gained during the project laid a foundation for this more extensive background research project funded by the City of Helsinki. The European Centre of Excellence for Countering Hybrid Threats, founded in Helsinki, provided background support and supervision for the report. The writers would like to thank the Hack for Society project and its implementers: Helsinki Think Company, the University of Helsinki, the Ministry of Education and Culture, Sitra, the Association of Finnish Local and Regional Authorities, the e2 think tank and, of course, the City of Helsinki and everyone who participated in the project as well as the experts who gave us their time.

Introduction to hybrid influencing

Various political analyses often debate how much the operating environment of safety and security policy has changed. When talking about *hybrid warfare*, it is often stated that it is not something new as such and that its methods have been used before. On a general level, this is true. However, leaving the analysis at this level would be risky.

The development of technology, social trends and geopolitical positions has led to a change in the relative effectiveness of the methods and given them new forms. For example, social media combined with automatic algorithms creates completely new types of mechanisms for informational influence in the changed media field, even though informational influence as such has a long history.

Hybrid threats and hybrid influencing cover a variety of activities, and the terminology specifying them varies. In the following section, we will examine the background of the subject, its terminology and how hybrid threats must be prepared for, specifically at city level.

1.1 What are hybrid influencing and hybrid threats?

Hybrid influencing is conscious influence exerted by a party, utilising multiple influence methods in order to reach their goal. The purpose of hybrid influencing is to weaken and/or harm the target.

A hybrid threat is an embodiment of influence methods that has been deemed to be a threat. Hybrid influencing is characterised by obfuscation of the connection between the actor, the methods and the goals. The target of the threat faces difficulties discerning the boundaries of hybrid influencing or identifying who is responsible. The purpose of these activities is to be unidentifiable at the start, and if the activities are ever discovered and/or identified, the actor will not admit them. The aim is to carry out these activities in the middle ground between war and peace in order for countermeasures to be as difficult as possible. However, it is worth noting that protecting ourselves from hybrid influencing does not always require such a situational overview: it is more important to identify our own vulnerabilities and know the various consequences, including indirect ones, of our own measures. In fact, hybrid influencing is often based specifically on the utilisation and maintenance of existing vulnerabilities and weaknesses.[1]

The European Centre of Excellence for Countering Hybrid Threats has divided hybrid threats into two phases: Figure 1 illustrates hybrid influencing and hybrid threats. In the priming phase, the influencer makes preparations for hybrid influencing by creating or identifying channels for exerting influence. In practice, this means observing and creating various vulnerabilities, practising their use, testing their impacts or using them as a diversion. In the operational phase, the influencer seeks to achieve its objective by combining various methods. If the selection of methods extends to the use of military force, we can talk about hybrid warfare. This report does not address hybrid warfare; instead, it focuses on combinations of methods other than military methods.

As stated above, a key characteristic of hybrid influencing is the obfuscation or concealment of various phases and connections. In the context of Russia's activities, hybrid influencing has sometimes

1) According to the European Centre of Excellence for Countering Hybrid Threats, a hybrid threat can be characterised as coordinated and synchronised action that deliberately targets the systemic vulnerabilities of democratic states and institutions through a wide range of methods. The activities exploit the thresholds of detection and attribution as well as the border between war and peace.
The aim is to influence different forms of decision-making at local (regional), state or institutional level to favour and/or gain the agent's strategic goals while undermining and/or hurting the target

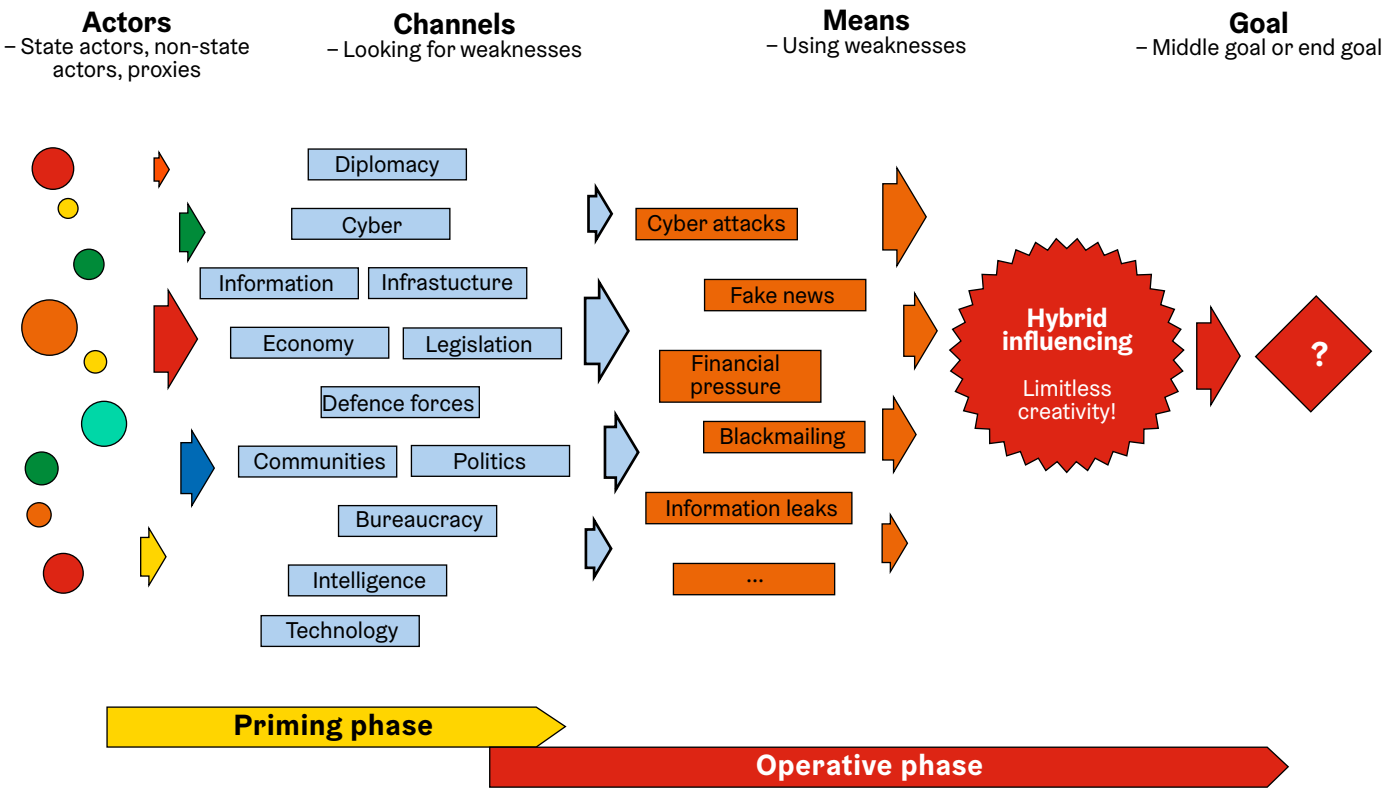

Photo 1: Hybrid influencing as a diagram. (Source: HybridCoE, edited)

been compared to a game of chess. In reality, poker would be a better analogy, as its key characteristics include bluffing and taking advantage of random opportunities.

Methods of influence may for example include informational influence, financial influence, physical influence, political influence and cyber operations as well as political violence. With regard to the breakdown of methods, it should be noted that an activity can simultaneously be more than one of these. For example, if all operations utilising the Internet are classified as cyber operations, then they can all be cyber operations while simultaneously being perceived as informational influence, for instance. Similarly, informational influence can be linked to political influence, such as turning the consequences of a particular law against the state that enacted it.

In a democratic society, political decision-making and the opinions of residents are influenced. Various methods are also combined in order to reach the objective of influencing more effectively. This is a normal, deliberative political activity. Just as there is social or communicative influence that cannot be classified as a threat, there is also governmental influence, i.e. diplomacy.

However, influence may sometimes be a threat. Classifying something as a threat constitutes normative classification: a threat is something unwanted, i.e. something that is deemed to be wrong or evil. Threats can often easily be classified in the legal sense: in many cases, they are a criminal activity. From the perspective of a municipality – in the context of this report, Helsinki in particular – harmful influencing targeted at critical operations is a clear threat. Critical operations refer to the infrastructure, processes and organisations necessary for the city's basic operations as well as, possibly, some individuals (MCDC: 11). According to the classification by the Ministry of Transport and Communications, critical operations include the sectors of energy, transport, banking, financial market infrastructure, health care, drinking water supply and digital infrastructure (Working group supporting the implementation of the Directive on security of network and information systems 2016). Threats can also be assessed based on whether they are primarily perceived threats (subjective threat) or systematically assessed threats (objective threat).

Talking about hybrid influencing does not mean that individual methods of influence cannot be discussed. A possible combination of methods in regards to the timing and/or objective is possible to identify as long as we first understand what the individual methods are. In this report, various methods of influence are discussed in the context of hybrid influencing, even if we only talk about individual methods or operations.

The use of individual methods or a combination of multiple methods may be implemented by a govern-

mental or non-governmental actor. The actor may also be an individual or an organisation with some type of connection to a particular state.

In other words, the terminology of hybrid influencing is not uniform, even among Finnish authorities or experts. Some contexts emphasise the combining of methods in particular, while others treat individual methods of influence, such as informational influence or cyberattacks, as hybrid influencing. However, we must also note here that the overall security of Finland rests on a strong foundation. Examples of this include the Security Strategy for Society (2017), the national risk assessment (2015) as well as the Ministry of the Interior's research project on the interdependence of internal and external safety and security (2016). Many of the challenges noted in this report have been identified. The challenge is that hybrid influencing taking place in the safety and security environment of today is constantly creating new and changing threats.

1.2 Hybrid influencing and responding to it at local level

For the purpose of this report, an online survey was conducted among the members of Helsinki City Council in autumn 2017. The 17 council members who replied undoubtedly do not comprehensively represent the entire council, but their replies presented some interesting views. Social exclusion and inequality were the most common things mentioned as threats, but climate change, terrorism and extremist groups were also mentioned. When identifying actors that pose a threat, Russia was mentioned alongside radical groups. Dramatic influence like a cyberattack or an act of terror was found to be a greater threat than less visible activities such as financial pressure or corruption.

The council members expressed a range of views about the foreign policy dimension of local politics of Helsinki. Foreign policy was considered as influencing the decisions made in Helsinki, but the respondents did not agree on how local decisions can impact national politics and thereby foreign policy. Ignoring this dimension may pose a risk – local-level decisions or political situations may unknowingly create vulnerabilities and opportunities for third parties to exert influence. For example, many of those working in the City of Helsinki Group may also be active at national level. This makes it possible for impacts that start at local level to extend to national level.

The responses of the council members reflect the common view that hybrid influencing is perceived as a state-level activity: One state influences the position or actions of another state. However, when examining the range of methods used in hybrid influencing (see Figure 1) it is apparent that the local level plays a highly significant role as both a target of influence and in preparing for it. Critical infrastructure as well as activities or people targeted by influence are always located somewhere, and a local actor is often at least indirectly responsible for safeguarding the activities of society.

The role of the local level in hybrid influencing is increased further by the global urbanisation trend. Today, more than a half of the world's population lives in urban areas (UN, 2014). Challenges to sustainable development, such as climate change, financial inequality and refugees, are largely solved in cities specifically (UN-HABITAT, 2016). Cities are also perhaps increasingly becoming focal points of social tensions, and individual places in them may gain an enormous symbolic status in social movements. Examples of this include Tahrir Square in Cairo and Maidan Nezalezhnosti in Kiev, which have played key roles in uprisings (MCDC, 2017). This simultaneously increases cities' role as targets of hybrid influencing.

In other words, responding to hybrid threats is largely in the hands of municipalities. Many municipalities have begun preparing and practising for hybrid threats. A possible challenge is that municipal services are increasingly provided together with individual service providers, based on agreements. This inevitably forces us to think about the city's possibilities for independent preparedness. Most likely, cities will have to work in closer cooperation with their contractual network with regard to preparedness. Helsinki's role as Finland's capital is particularly emphasised, as a large amount of the economic and political power in the country is concentrated in Helsinki. By influencing Helsinki, one can influence the entire country, and Helsinki can improve the security of Finland by being well-prepared.

Photo 2. Source: Helsingin kaupungin aineistopankki, Pertti Nisonen, 2017.

In Finland, the significance of the local level is emphasised by the broad self-government of municipalities and their responsibility for public services. A considerable proportion of the political decisions that affect people's everyday lives are made by municipal boards and councils, and municipalities are in charge of social services, health care and education, for example.

These sectors are not only potential channels for exerting influence, but they also play a key role in the response to hybrid threats. Citizens' trust in each other and official institutions has a major impact on society's susceptibility to hybrid influencing and society's resilience in the event of disruptions after the realisation of a threat. The role of the local level is highlighted in building and maintaining trust; municipalities often provide a face for public administration. Even though not all safety and security authorities are subordinate to municipalities, their operations also involve building trust and collecting information at local level.

1.3 Classification of hybrid threats

Hybrid influencing and threats can be broken down in various ways. The multinational MCDC project (Cullen & Reichborn-Kjennerud, 2017) divided the methods of hybrid influencing into *military, political, economic, civil* and *informational* instruments of power. Similarly, the influence activities may target political processes, military targets, the economy, dissemination of information or infrastructure.

This type of breakdown of targets and methods is a useful way to analyse the actors, influence channels and responsibilities in preparedness efforts that are targets of influence. However, the problem in this is that this type of examination may direct too much attention to individual operations of society and direct influence mechanisms, thereby possibly obscuring the overall threat posed by combinations of mechanisms.

Hybrid influencing can also be divided according to the nature of the activity. This makes it possible to identify the influencer's goals, such as:

- *Creating or maintaining a vulnerability*, with the influencer building the range of methods at its disposal based on a particular vulnerability. The vulnerability forming the threat may just as likely be technical, economic or human in nature. An example of such an activity would be supporting a fake news website.
- *Observation*, in which the influencer collects information about the target or the target's activities in relation to some other threat or development.
- *Testing*, in which the influencer tests the target's actions, reactions or the consequences of a particular method. An example of this would be cyberattacks that test the capabilities and weaknesses of IT systems.
- *Practising*, in which the influencer tests and practises its own range of methods.
- *Diversion*, in which a particular method of hybrid influencing is utilised to direct attention away from some other activity.

When assessing threats, it should be noted that the perceived threat and actual threat do not always match. However, overreacting to a minor or non-existent threat may make the threat real. For example, treating a particular population group as a risk may sow distrust and lead to juxtaposition, ultimately radicalising a part of this population group. On the other hand, ignoring threats that are perceived as significant but that authorities assess as minor may cause distrust towards the authorities – in this context, communication and open interaction play a key role.

Helsinki as a target of influence and as an actor

Many of the structures that expose us to or protect us from hybrid threats are created at local level. As the capital of Finland, Helsinki is also in a special position with regard to preparedness for hybrid influencing. In the following section, we will first examine the preparedness of the City of Helsinki Group for hybrid threats and then consider the city's susceptibility to various forms of influence. Various possible forms of hybrid influencing are also presented in Appendix 1.

2.1 City of Helsinki Group's preparedness for hybrid threats

According to the City Stategy, Helsinki is safe and pleasant, smooth, easy and caring (City of Helsinki, 2017b). The City of Helsinki Group's safety and security efforts are steered and determined by a wide range of documents. The City Strategy (City of Helsinki, 2017b) steers all operations of the city. The most essential policies of the strategy that steer safety and security efforts are the City of Helsinki's safety and security principles (City of Helsinki, 2017a), organisational safety and security policies (City of Helsinki, 2017c) as well as the previously prepared Preparedness regulations (Vuosalmi, 2015), Safety plan (City of Helsinki, 2015), Principles of local safety planning (City of Helsinki, 2014) and Internal control and risk management regulations (City of Helsinki, 2015b).

These documents outline the city's general model for leading and managing safety and security. The city divides safety and security into three levels: the strategic level, which is addressed in the City Strategy; the city level, which is addressed in the aforementioned plans and instructions; and the residential area specific level, which is steered by site- and area-specific plans (City of Helsinki, 2014). In general, the responsibilities are divided so that the city manager is in charge of the City of Helsinki Group's safety and security management, while the Safety and Preparedness Unit steers and coordinates safety and security matters within the Group and with interest groups; the premises security manager from the Buildings and Public Areas Unit is in charge of the safety and security of properties and premises together with the City of Helsinki Executive Office; and the responsible persons of sectors and municipal enterprises are in charge of their own operations (City of Helsinki, 2017c). Documents that steer safety and preparedness efforts and their planning are regularly updated, with the updating process underway even now.

Helsinki has a multidisciplinary approach to safety and security. Cooperation is also close with interest groups outside the City of Helsinki Group: for example, permanent cooperation structures have been established with the police, and the city is an increasingly active participant in preparedness drills organised by the Finnish Defence Forces.

2.2 Cyberattacks and critical infrastructure

Digitalisation has also highlighted the role of individuals in threats posed to infrastructure. If the monitoring and restricting of access to information or premises is weak, an individual person may quickly cause a great deal of damage either unknowingly or on purpose. Cyber and facility security is never only a matter of technology; the processes and the competence of personnel must also be up to date.

Digitalisation has significantly increased our dependency on functional information systems. These dependencies make us susceptible to disruptions even without deliberate influence. An illustrative example of this is the replacement of the Oriola information system in 2017, which caused serious long-term problems for the pharmaceutical services of the whole country. Depending on the nature and criticality of the operations, various organisations should test and practise situations in which key information systems do not work as expected. This type of 'day without Internet' may in practice be an extremely expensive test, and maintaining substitute arrangements may in some cases not necessarily be cost-ef-

Photo 3. Source: REDPIXEL.PL/Shutterstock.com.

Computer networks and infrastructure are also obvious targets of influence in Helsinki. Influence that takes advantage of computer networks is referred to as cyber influence. With the advancement of digitalisation, practically all operations in society are somehow susceptible to cyber reconnaissance or cyberattacks.

However, critical infrastructure can still be further threatened by other methods, and physical reconnaissance, for example, is known to occur continuously. There are known cases in the Finnish municipal sector in which critical infrastructure facilities have been physically accessed by external persons. Infrastructure and computer networks can also be accessed by financial, fully legal means, such as through direct ownership or by obtaining control of contracts or projects of actors who are responsible for infrastructure. According to the experts interviewed, the security leak that resulted from the outsourcing of the Swedish Transport Agency (see for example Sveriges Radio, 2017) and the procurement of plots and properties near strategic sites in Finland are examples of such a vulnerability. Municipal actors must therefore know their contractors, while the contractors must know their own social significance.

fective. Regardless, the minimum requirement should be for organisations to be aware of their dependency on information systems and be prepared to act in the event of a disruption. At present, we often place too much trust in the functionality of systems. On the other hand, the threats posed by disruptions in data communications are now recognised better, and a cyber security drill known as Tieto 2018 was launched at the initiative of the National Emergency Supply Agency, intended in particular for companies that are critical to the security of supply (National Emergency Supply Agency, 2018).

The City of Helsinki and operators that are important to the city use an enormous variety of information systems, in addition to which an increasing number of organisations, employees and elected representatives utilise external, commercial applications and platforms (such as Facebook, Twitter, LinkedIn, Instagram, WhatsApp, Slack, Office 365 and email applications) in the performance of their duties. The diversity and overlap of the systems makes it impossible to form a comprehensive overall picture, which highlights every individual's responsibility for their own actions. In addition to data leaks and other cyber influence, social media in particular can be utilised in smearing the reputation or competence of an operator. For example, a photo published on social media may show an employee's access pass, which is easy to copy if someone wants physical access to premises.

The City of Helsinki is also a significant employer and payer of wages and benefits. Financial administration is a potential target for cyber influence, and people's livelihoods can also be viewed as a critical factor. The financial activities of the municipali-

The most essential infrastructure in Helsinki is related to energy, transport and water supply. Automatic systems connected to the Internet are potential weaknesses in such technical systems. Extensive or long-term disruptions in electricity, water or heat distribution would cause serious problems, while disruptions in public transport would cause great harm, and disruptions at ports could at worst result in national financial losses. In Helsinki, these operations are primarily managed by the City of Helsinki Group or joint municipal authorities, which presumably streamlines joint preparedness and communication at local level. The same thing largely applies to social and health care services. However, joint operations and communication do not happen by themselves – they require operating methods to be planned and practised.

These limited companies are not automatically obligated to prepare for threats, which means that the municipalities that own them must use steering to ensure their preparedness.

Photo 4. Source: Helen Oy.

Photo 5. Source: Helsingin kaupungin aineistopankki/ Kuvasuunnittelu- ja Agentuuritoimisto Keksi 2014.

A hostile actor can combine cyber methods with physical influence. A cyber operation can be used to edit patient data, i.e. tamper with the data's integrity. In the context of cybersecurity, integrity refers to data being edited only by persons who have the right to edit it. If the cyber operation was not detected, people would trust in the data's integrity and act accordingly. This could have concrete and substantial physical consequences: a cyber attacker could affect people's health by causing doctors to make incorrect treatment decisions based on false patient data.

ty's residents, such as buying food, are made difficult if wages or benefits are not paid. Payment transactions would also cease in the event of a disruption in the supply of electricity. As is characteristic of hybrid influencing, this type of disruption would be particularly serious if combined with other methods, such as informational influence. Dissatisfaction with the authorities and decision-makers would increase. The situation could affect decision-making in a way that would harm Helsinki.

Another type of cyber method is the misuse of rights granted under legislation. For example, the EU's General Data Protection Regulation provides people with the right to request that organisations that collect information about them provide them with this information. The regulation could be taken advantage of in a denial-of-service attack by flooding the targeted organisation with thousands of data requests. The organisation is obligated by law to respond to every request. This type of situation can be achieved with informational influence operations: a hostile actor feeds disinformation that becomes newsworthy and uses social media to produce and generate information. In this hypothetical example, it is claimed that the organisation in question is processing data incorrectly. The hostile actor could appeal to people's emotions in order to persuade as many people as possible to request their data within a short period of time. It could make a false claim, such as that data concerning children is somehow being misused or used dubiously by the organisation. Similar obligations that make organisations susceptible to threats can arise when outlining various service promises.

2.3 Administration and decision-making

In Finland, municipalities have extensive obligations and self-government. Municipal administration and decision-making are thereby also potential targets of hybrid influencing. By influencing them, a hostile actor could significantly advance their position or objectives. The preparedness efforts of Helsinki are discussed above in chapter 2.1. Hybrid influencing is not directly addressed in Helsinki's public documents, but the multidisciplinary perspective of the city towards safety and security in itself creates the conditions to prevent these threats better than a narrow definition of safety and security that is based on silo mentality.

The city's public documents do not contain exact threat assessments or individualised analyses of operators. The safety and security efforts also have limited connections to the city's highest decision-making body – the City Council – and other political elected bodies, and possible exertion of influence through the political system has not been examined as a risk. The political system can be considered to be particularly susceptible to influence at municipal level. Elected representatives primarily perform their duties while working full time. There are large differences between council members and between council members and office holders in their level of knowledge and familiarity. At worst, the situation enables the misuse of an office or elected position if a hostile actor succeeds in manipulating an individual decision-maker.

By influencing municipal decision-makers, it would be possible to advance a building permit process, for example. Promoting your own interests is not wrong as such – it is usually called lobbying. For the municipality and society, this could be classified as a threat if it constitutes a crime or an activity that has indications of influence that undermines security. An example of this would be a situation in which an applicant for a building permit says that they run a business that is in reality a coverup for influence that undermines security. In such situations, the facade of the activity can be kept clean, making it difficult for internal safety and security authorities to uncover the actual nature of the activities.

In Finnish society, administration is largely decentralised, both regionally and in terms of operations. The risk in this type of model is uncertainty about responsibilities and leadership in rapidly progressing situations – on the other hand, it also enables flexible local action. A decentralisation of operations is highlighted in Helsinki, and it requires precise planning and practice for potential disruptions in order to ensure the clarity of roles and responsibilities. For example, telecoms operators are meant to notify the Ministry of Transport and Communications if they suspect that they have been the target of a data breach (Working group supporting the implementation of the Directive on security of network and information systems, 2017). However, many of the interviewees doubted whether the notifications submitted to different bodies could be linked to each other if necessary.

In today's operating environment, assigning responsibilities is challenging in external communications in particular, as various fast-paced communication channels are difficult to control in a centralised way. Smooth communication between the city and various governmental operators is essential. A quick assessment of the situation, consideration and uniformity of communications inspire trust and help prevent communication itself from escalating the situation by making room for false information or by emphasising juxtaposition.

Mutual dependencies within and outside the city organisation must also be known well in order for preparedness to be realised according to plans. Some of the experts we interviewed brought up the fact that these dependencies are not yet known well enough.

The new leadership model and sector structure of Helsinki have also brought clarity to the city administration from the perspective of preparedness. This change is perceived to have improved the city's preparedness and clarified the division of responsibility in preparing for disruptions. In addition to a functional division of responsibility, preparedness for hybrid threats also requires ensuring that someone is responsible for the overall situation and can recognise the combined consequences of different influence methods if necessary. Here, the division of responsibility must be sufficiently seamless between regional and state levels.

Several of the interviewees stated that stronger leadership is required to prevent hybrid influencing. Some felt that the theme of hybrid influencing is currently no one's responsibility, instead being sprinkled across the agendas of various organisations. Because of this, potential influence methods may not necessarily be able to be linked to each other. Among other things, it was proposed during the interviews that the Ministry of Transport and Communications could be assigned the role of coordinator. Another option would be a municipal level security ambassador who would actively bring up changes and new challenges in the safety and security environment and coordinate the dissemination of information at local level, between different local levels as well as between local level and the state.

A hasty or poorly prepared policy may by itself make the decision-making process susceptible to vulnerabilities. For example, the uncertainties and lack of clarity related to the regional government, health and social services reform make preparedness planning difficult. If the extensive reforms involve a redetermination of responsibilities and upgrading information systems, this process will require special care. In particular, it must be ensured that security will not be compromised during the transition period and that the change will not create flaws in security.

Photo 6. Source: FGC/Shutterstock.com.

Elections are another potential target for influence. In some situations, an external influencer could wish to influence the outcome of an election in order to pass decisions beneficial to the influencer or create a political setting that would weaken the decision-making ability. However, the objective may simply be to undermine trust in the system: if external influence takes place right before an election, it can weaken trust in a democratic election outcome, particularly if the influence is revealed after the election.

Photo 7. Source: Cigdem/Shutterstock.com.

Trust is a key variable in protection against hybrid threats. Social trust promotes a sense of security and facilitates cooperation and interaction. Social trust means that people trust each other, the structures of society and the authorities. All of this improves our ability to prepare and protects many critical operations. Trust is therefore one of the targets of informational influence.

Successful information influence can weaken trust and thereby enable the use of other hybrid methods. The 'filter bubble effect' accelerated by current communications platforms is an opportune growth platform for the polarisation of discourse. Polarisation feeds distrust. The notion that there are only two extremes in some matter strengthens the activities of the external influencer and/or may be a consequence of it. This type of influence can take place over a long period of time, and its effects may not be felt until after a long delay.

2.4 Information and trust

The target of hybrid influencing does not always have to be any clear operation of society. Hybrid influencing may just as well target social communications, trust and the opinion environment. This type of influence is often described as *informational influence* – it was also referred to as psychological warfare, particularly in the past. However, information may not necessarily be the tool used for psychological influence, as an attention-grabbing criminal activity or act of terror, for example, may be used to weaken trust in the authorities or lower the general sense of security.

The sense of security of the residents of Helsinki is studied regularly, and the residents perceive the city centre and their own residential areas to be relatively safe – though there are clear differences between some areas. At the same time, as somewhat of a contradiction to this, the general security situation is assessed as weakening. This is probably rooted in the contradiction between people's own experience and the image conveyed by the media. The future of children and young people, terrorism, climate change, increasing income disparity, wars and military conflicts are what concern the residents of Helsinki the most in the most recent security study. More than half of the respondents considered these to be at least somewhat concerning. (Keskinen & Laihinen, 2017.)

The city is often the face of public administration at local level. Helsinki must ensure that it has the trust of its residents, and openness and interaction play a key role in these efforts. The city's core mission is to provide its residents with a comfortable environment and services, but mental images and communications also have major significance in the establishment of subjective experiences today.

One of the challenges faced by the city is connecting with various residents who are difficult to reach, such as linguistic minorities. Local communities, non-governmental organisations and foundations can serve as good channels for engaging in interaction with linguistic minorities. However, representatives of linguistic minorities or other population groups should not be marginalised and left to these operators. It is also important to be aware of the organisations' financing and goals. We need more forums for dialogue. According to a report by the Cultura Foundation (2017), many Russian-language organisations have the capacity to provide municipalities with integration services. However, challenges include the insufficient understanding of some organisations regarding their own role, linguistic and cultural challenges, overburdened employees and volunteers as well as a lack of funding, facilities and time. Additionally, some people are difficult to involve in the activities for various reasons. (Varjonen, Zamiatin & Rinas 2017.)

The tensions between various population groups are also vulnerable to hybrid influencing. If some part of the population feels that it has been marginalised, its representatives are more susceptible to becoming radicalised or recruited by an external party. In other words, a suspicious attitude towards a population group may feed distrust and increase the popularity of extremist movements, for example.

A representative of some population group may also be a target of influence for reasons largely unrelated to them. Examples include dual citizens and other persons with family ties or other close ties abroad (Ferm, 2017). Operating around these settings requires public administration to consider things very carefully, communicate in a professional manner and keep a keen ear to different perspectives. It is important to ensure that linguistic minorities and residents with a foreign background feel that they belong in the city as a community. This may not necessarily be the case at the moment.

For example, according to the Cultura Foundation's report (Varjonen et al., 2017) the risk of social exclusion is higher for Russian-speaking immigrants than the rest of the population, and experiencing discrimination makes it more difficult to identify with the majority population. This may create a foundation for influence that targets this part of the Russian population (Davydova-Minguet, et al., 2016), but in this case as well, overestimating the power of influence and treating this part of the population as a possible risk factor may pose threats. It is important to note that at present the Russian-speaking population of Finland appears to trust the Finnish authorities even more than the majority population of Finland does (Varjonen, Zamiatin & Rinas 2017, 49). This trust should be safeguarded.

In the everyday life of residents, the police has the most visible presence among the safety and security authorities, and a high level of trust in the police is a significant resource in Finland. The police are a national authority and is therefore not directly controlled by the municipality. However, the police are a significant local operator and authority, whose operations affect the perceptions of citizens. How safe people feel their city and municipality to be depends largely on their perception of the operations and importance of the police. There is a risk of trust in the police weakening.

Different extremist movements have different attitudes towards the operations of the authorities: some try to be juxtaposed with the police, while others emphasise the lawfulness of their activities. It may be in the interests of various parties to make the police out to be a supporter of either their own or the opposing side. This type of setting may be an attrac-

Photo 8. Source: Helsingin kaupungin aineistopankki/Aiko Lohtander 2018.

Not all internal and external safety and security authorities are subordinate to the city, but their local operations play a key role in building a sense of security and trust. Helsinki works in close cooperation with the police, the Finnish Defence Forces and the Finnish Border Guard. Helsinki's own significant safety and security operator is the Rescue Department, which is responsible for assessing and preventing risks of accident in the city and preparing for a variety of accidents, emergencies and emergency conditions.

tive place for informational influence, with the objective of inviting general suspicion and unrest. If the police are perceived to favour a particular perspective or side in polarised discourse, or if the police are perceived as a weak operator, this may lead to concrete activities in the municipality that threaten safety and security.

Young people are a special group from the city's perspective, as they can be reached directly through upbringing and education. Preventing social exclusion is an essential part of the city's safety and security efforts, and the school system plays a key role in this. In addition to providing opportunities that prevent social exclusion, it is important to develop young people's media literacy skills and the conditions for building trust.

At present, young people's perception of safety and security in Finland is relatively weak (Limnéll & Rantapelkonen, 2017). This is concerning, as a subjective experience can lead to a certain type of vicious

The school system can also be a direct target of influence. According to one interviewee, an actor can for example attempt to influence the content of education with different methods of disseminating information. Municipalities and privates schools prepare their own curricula based on national criteria. The objective of an actor that uses influence may, for example, be to increase positive attitudes towards itself or the target's susceptibility to its interests. The influence activities may, for example, target teachers, guardians, rectors, employees of the Education Division or members of the City Council. Once we become aware of this possibility, we can critically assess the decisions made in everyday situations and at the level of a strategic curriculum.

Photo 9. Source: Helsingin kaupungin aineistopankki, Kimmo Brandt 2015.

circle of insecurity when these young people transition to working life. However, one particular observation is that the young people in the Helsinki Metropolitan Area are geographically the only group in Finland to believe in the positive development of their personal safety and security. The young people in the Helsinki Metropolitan Area view polarisation and the distribution of the population to be the greatest threat (Ibid.).

In addition to having an educational mission, schools also build a sense of community. The communities formed at schools strengthen the sense of security and increase resilience, i.e. tolerance, to hostile external influence. This is why we need to pay special attention to well-being at schools. Schools provide children and young people not only with information on subjects and phenomena but also skills for being part of society. Trust in society and one's own municipality and city also develop at an early age.

In addition to the aforementioned groups and operations, influence can also increasingly effectively target individuals, achieving a greater impact with individual cases than their number would suggest. Targeted online harassment has become a recurring phenomenon, which is often rooted in some degree of systematic machination. When targeted at those who express some view or opinion, these activities can raise the threshold for participating in discourse and, for their part, poison the general atmosphere. Current legislation or its enforcement would seem to be an ineffective way to prevent these activities. An individual may also become a target of influence in other situations, or some activity may be polarised according to the interests of the influencer. An example scenario would be a situation in which the care of a patient with a foreign background fails for one reason or another. After this, the physician is placed in the spotlight and the individual is politicised at a higher level.

The media, which is responsible for independent dissemination of information, is a key operator in maintaining social trust. On the other hand, society is also built on the assumption that the media operates in a trustworthy manner. Fake news activities undermine this setting both directly by intentionally disseminating false or biased information and indirectly by taking advantage of society's openness and the position of reporters. For example, confidential communications or an event intended for reporters turns against its purpose if it involves fake reporters who are indifferent to the rules of journalism. On the other hand, social exclusion allows the situation to be presented as cooperation of the 'mainstream media' and the 'elite'. Linguistic minorities pose their own challenge, as biased media controlled by a foreign power may be more accessible to them than Finnish news coverage and communications. In addition to fake news, the dissemination of false information also utilises fake accounts of individuals and institutions online – even when implemented sloppily, these may be used to create confusion or simply divert people's attention elsewhere.

Preventing and taking protections against hybrid influencing that targets information and trust requires openness to be balanced and implemented carefully. On one hand, openness is an excellent way to build trust, and the transparency of public operations may also enhance it. On the other hand, openness allows it to be utilised to cause trouble.

In general, various categories and methods of influence can be recognised in fake news and disinformation (Nothhaft et al., 2018). News can be made up, its content can be manipulated and it can be made to be misleading. Direct propaganda, satire, parody and advertising can also be harnessed as tools of disinformation. Fake news can, for example, be used for the purpose of building a new narrative that defends a particular party, or it can simply be used to undermine the clarity and credibility of actual news and legitimate information (Nothhaft et al., 2018).

Photo 10. Source: Docstockmedia/Shutterstock.com.

Summary and conclusions

The purpose of this report is not to systematically assess the preparedness of Helsinki to hybrid influencing, list all the possible threats that exist or present comprehensive instructions for the future. The subject involves a great deal of confidential information, without which this type of assessment is, in any case, impossible. On the other hand, the nature of hybrid influencing involves surprise and continuous change: a precise list of the methods observed and considered so far can become outdated tomorrow. The purpose of this report is to improve awareness and understanding of the topic among non-professionals (such as members of municipal councils and authorities in the various sectors of Helsinki) and present terminology that clarifies the subject. These by themselves help to prepare for hybrid influencing and hybrid threats better.

In other words, hybrid influencing is goal-oriented influence that is exerted by an external actor by utilising various methods and that is harmful to its target and characterised by the obfuscation of the links between the actor, the methods and the objective. State-level operations are often highlighted in the management of internal and external safety and security, but the local level – municipalities and cities – are not only targets of influence but they also control many methods for protecting themselves against threats.

A target of hybrid influencing may just as easily be 'hard', such as a port or power plant, or 'soft', such as social cohesion. These are also not mutually exclusive. Finnish society is, as such, well-equipped to protect itself from hybrid influencing. A long-standing culture of overall safety and security and preparedness, as well as high social trust, are assets in these efforts, but it is important to ensure that the operations at local level tie into the big picture.

Communications and cooperation should be smooth and continuous between the city and various organisations, among the city's residents and communities as well as between the city and state-level operators. The responsibility for the overall situation and monitoring various methods of hybrid influencing must be at a sufficiently high level.

Ultimately, the city's most significant influence opportunities can be found specifically in the building of trust. Among the parts of public administration, the city is often the closest to the individual and thereby has many opportunities to increase residents' trust in the official machinery – and each other. This role must be internalised across the City of Helsinki Group. For example, experiences of the city environment, upbringing and education or social and health services contribute strongly to the atmosphere which we live in and which can be undermined by hybrid influencing.

The key would be for the city to establish a profile for itself in relation to its residents in order to make the link between the city administration and the residents in everyday life visible. Building a sense of community is important. It provides a strong countermeasure to hybrid influencing. For example, upholding school communities would be important.

Finally, it should be noted that not all negative things have malicious hybrid influencing behind them. We are also able to create problems for ourselves without external assistance. If we fear hybrid influencing at every turn, the suspicion itself can destroy trust and provoke various parties. Rather than overemphasise matters, it is wiser to understand and be aware of the nature of hybrid influencing and the possible interests of various parties. It would be wise to weigh these matters in the background in the development and running of the city. Actions that promote protection against hybrid threats also often provide other benefits. Developments that make us susceptible to hybrid influencing, such as social tensions and mutual distrust, should be contained in any event.

Sources

The report is largely based on expert interviews (18 interviews). Due to confidentiality issues, the information from the interviews is not cited.

The organisations where the interviews were conducted:
National Emergency Supply Agency, Media pool of the National Emergency Supply Organisation, National Bureau of Investigation, KPMG, Finnish Border Guard, City of Helsinki, The Hospital District of Helsinki and Uusimaa, Aalto University, Faktabaari, Cultura foundation, Southern Finland Regional State Administrative Agency, CGI.

Cullen, P.J. & Reichborn-Kjennerud, E. (2017) MCDC Countering Hybrid Warfare Project: Understanding Hybrid Warfare, MCDC, January 2017.

Davydova, O., Sotkasiira, T., Oivo, T. & Riiheläinen, J. (2016) Suomen venäjänkieliset mediankäyttäjinä. (Finland's Russian-speakers as media users.) Publications of the Finnish Government's analysis, assessment and research activities 35/2016. [URL: http://tietokayttoon.fi/documents/10616/1266558/Suomen+ven%C3%A4j%C3%A4nkieliset/0265446a-afd4-4c51-92dc-2d16350ac8c7?version=1.0]

Ferm, T. (2017) Laws in the era of hybrid threats, HybridCOE Strategic Analysis December 2017. [URL: https://www.hybridcoe.fi/wp-content/uploads/2018/01/HybridCoE_SA_2017_Dec_Ferm.pdf]

City of Helsinki (2014) Paikallisen turvallisuussuunnittelun periaatteet Helsingissä. (Principles of local safety and security planning in Helsinki.) City of Helsinki Executive Office 16 May 2014. [URL: https://dev.hel.fi/paatokset/media/att/87/87314098c7cffc69ba7f8836049f30314ced9258.pdf]

City of Helsinki (2015a) Helsingin kaupungin turvallisuussuunnitelma. (City of Helsinki safety and security plan.) City of Helsinki, publications of the Central Administration 2015:28 [URL: https://www.hel.fi/static/kanslia/Julkaisut/2015/Helsingin_kaupungin_turvallisuussunnitelma.pdf]

City of Helsinki (2015b) Sisäinen valvonta ja riskienhallinta Helsingin kaupunkikonsernissa. (Internal control and risk management in the City of Helsinki Group). Instructions by the City Board 16 October 2015. [URL: https://dev.hel.fi/paatokset/media/att/f2/f28de5f5f3e95725161ed8c653608d1e8a543cd6.pdf]

City of Helsinki (2017a) Helsingin kaupunkikonsernin turvallisuusperiaatteet. (Safety and security principles of the City of Helsinki.) City of Helsinki Executive Office 17 January 2017. [URL: https://www.hel.fi/static/public/hela/vipa11010VH1J_Kaupunginjohtaja-J/Suomi/Paatos/2017/Kanslia_2017-02-01_Kj_14_Pk/C5D038D8-E226-CE06-8584-59AD8A400000/Liite.pdf]

City of Helsinki (2017b) Maailman toimivin kaupunki – Helsingin kaupunkistrategia 2017–2021 (The Most Functional City in the World: Helsinki City Strategy 2017–2021). [URL: https://www.hel.fi/helsinki/en/administration/strategy/strategy/city-strategy/]

City of Helsinki (2017c) Organisaatioturvallisuuden linjaukset – Kaupunkikonsernin organisaatioturvallisuusohje. (Organisational safety and security policies – the City of Helsinki Group's instructions for organisational safety and security.) City of Helsinki Executive Office 18 May 2017. [URL: https://dev.hel.fi/paatokset/media/att/89/89c4730a6ae37e205123e9055edd25d44840c168.pdf]

National Emergency Supply Agency (2018) Tieto 2018 -kyberturvallisuusharjoitus käynnissä – Verkostona kyberuhkia vastaan, (Tieto 2018 cybersecurity drill underway – As a network against cyber threats.) [URL: https://www.huoltovarmuuskeskus.fi/tieto-2018-kyberturvallisuusharjoitus-kaynnissa-verkostona-kyberuhkia-vastaan/], Retrieved 11 March 2018.

Keskinen,V. & Laihinen, E. (2017) Kaikesta huolimatta turvallista – Helsingin turvallisuustutkimus 2015 (Safe despite everything – Safety and security study in Helsinki), Studies by the City of Helsinki Urban Facts 2017:2. [https://www.hel.fi/hel2/tietokeskus/julkaisut/pdf/17_04_05_Tutkimuksia_2_Keskinen_Laihinen.pdf]

Limnéll, J. & Rantapelkonen, J. (2017) Pelottaako? Nuoret ja turvallisuuden tulevaisuus (Are you afraid? Young people and the future of safety and security), Docendo.

MCDC (Multinational Capability Development Campaign) (2017) MCDC Countering Hybrid Warfare Project, Hybrid Warfare and its Countermeasures, Information note 2, December 2017.

Nothhaft, H., Pamment, J. & Agardh-Twetman, H. (2018) Countering Hostile Influence: the State of the Art, Research Report. (unpublished)

Sveriges Radio (2017) Government under fire after Transport Agency data breach, news 18 July 2017. [URL: https://sverigesradio.se/sida/gruppsida.aspx?programid=2054&grupp=24169&artikel=6740394]

Tiimonen, H. & Nikander, M. (2016) sisäisen ja ulkoisen turvallisuuden keskinäisriippuvuus (Interdependency of internal and external safety and security), Publications of the Ministry of the Interior 34/2016.

Yhteiskunnan turvallisuusstrategia (Security Strategy for Society), Resolution of the Finnish Government/ 2 November 2017, The Security Committee.

UN (2014) World Urbanization Prospects - Highlights, 2014 Revision. [URL: https://esa.un.org/unpd/wup/publications/files/wup2014-highlights.pdf]

UN-HABITAT (2016) Urbanization and Development: Emerging Futures. World Cities Report [URL: https://unhabitat.org/wp-content/uploads/2014/03/WCR-%20Full-Report-2016.pdf]

Vainio, T. et al. (2016) Suomen kansallinen riskiarvio 2015 (Finland's national risk assessment), Publications of the Ministry of the Interior 3/2016.

Varjonen, S., Zamiatin, A. & Rinas, M. (2017) Suomen venäjänkieliset: tässä ja nyt – Tilastot, tutkimukset, järjestökentän kartoitus (Finland's Russian-speakers: here and now – Statistics, studies, analysis of the organisational scene). Cultura Foundation.

Working group supporting the implementation of the Directive on security of network and information systems (2017), Directive on security of network and information systems. Final report of the working group supporting national implementation, Publications of the Ministry of Transport and Communications 9/2017.

Vuosalmi, Anssi (2015) Helsingin kaupunkikonsernin varautuminen ja jatkuvuudenhallinta – JULKINEN OSA. (Preparedness and continuity management by the City of Helsinki Group – PUBLIC PART.) [URL: https://www.hel.fi/static/liitteet/kanslia/Helsingin%20kaupunkikonsernin%20valmiusohje%20Osa%201.pdf]

APPENDIX 1

This table lists possible methods of hybrid influencing that were brought up during the background research for the report. The examples are hypothetical and do not necessarily refer to any observed activity.

Method	Purpose	Target	Examples	Preparedness methods
INFORMATIONAL INFLUENCE				
Influencing curricula	Establishing a positive attitude towards the actor and/or creating a juxtaposition between population groups (language, religion, history)	Local decision-makers, Education Division, students and guardians	Attempting to weaken the position of Swedish in education.	Awareness of the phenomenon Creative teaching solutions in culturally bound subjects Integrated teaching groups and teaching
Influencing municipal elections	Reducing faith in a democratic election result, promoting favourable candidates, creating juxtaposition, weakening decision-making	Voters, candidates	Financing selected candidates. Hacking the electronic voting system.	A protected (paper) voting system Openness of election funding
Local fake news	Creating a juxtaposition, 'creating a local reality', wounding the city's public image, distrust, crippling decision-making	City residents, local decision-makers	Utilising real or made-up local events in fake news, such as linking a crime to a particular population group or terrorism.	Improving media literacy skills in education Smooth and uniform operational communications that do not create a vacuum for false information Desire and ability to address difficult and politically sensitive topics in communications Openness
Association activities financed from abroad	Collecting information, maintaining a network of influencers, psychological influence, identifying vulnerabilities	Local, linguistic or cultural population groups, political movements, interest groups	Founding or running a seemingly non-profit organisation and using it to seize the interest representation and 'voice' of a population group. Utilising associations in disseminating disinformation.	Supporting the activities of trustworthy associations Services available in the resident's own language, opportunities to provide feedback and receive information Comprehensive representation of various population groups in decision-making and public discourse
Foreign or local medias financed from abroad	Informational influence, preventing integration	Population with a foreign background, linguistic and cultural populations	Local foreign-language radio channels and online medias. Political misuse of the position of reporters.	Local medias produced by minorities themselves and supporting these medias Comprehensive foreign-language communications of the public administration
CYBER INFLUENCE				
Toppling the public administration's information system	Creating distrust and uncertainty, making room for one's own message, financial benefits	The city's information systems	Disrupting the city's payment of wages via the information system.	Systematic information security Contingency plans
Breaching the city's databases and leaking information	Collecting information, creating distrust and uncertainty, financial benefits	The city's information systems	Hacking the client data of the city's social and health care services, blackmailing people with them.	Systematic information security Contingency plans Thought-out and confirmed procurements and outsourcing

Crippling/disrupting critical infrastructure with a cyberattack	Distrust, uncertainty, testing capabilities	The city's critical operations (water, electricity, heating, automated transport)	Disrupting the power supply in the city.	Cooperation of key organisations Improving the preparedness of households and increasing awareness
Congesting public services	Creating disorganisation, diverting attention	The city's information services	Using the data protection legislation to congest the services of the authorities.	Technical preparedness for large numbers Preparedness for communications in exceptional situations
PHYSICAL INFLUENCE				
Physical reconnaissance	Collecting information, creating threat scenarios, display of power, identifying vulnerabilities, practising	Secure facilities within the city.	Infiltrating secure facilities with false access rights.	Increasing awareness about risks Control and supervision of access rights
Drones	Collecting intelligence, physical attack, creating an atmosphere of fear, diversion	Critical targets, public facilities and areas (parks)	Flying drones in public areas in order to disturb and divert the attention of the authorities.	No-drone zones Legislation for control, such as police powers Taking drones into account in urban planning
Protests	Creating disorganisation, diverting attention elsewhere, polarisation, weakening the sense of security	Local linguistic and cultural population groups, political movements, interest groups	Supporting or escalating protests by extremist organisations, supporting opposing extremist movements to increase unrest.	Preventing social exclusion Close contact between the police and the city
Taking advantage of vulnerable individuals	Collecting information, gaining rights, radicalisation	Anyone, dual citizens, socially excluded people	Radicalisation and guiding of a socially excluded individual, blackmailing an individual in a critical position.	Preventing social exclusion Background checks and management of people-related risks
FINANCIAL INFLUENCE				
Real estate ownership	Crippling the infrastructure, political pressure, 'base of operations', a method to exert pressure	Properties across the city, properties near critical operations or infrastructure.	Property deals near a power station or water treatment plant.	Identifying critical operations and chains
Ownerships of other companies				Restrictive legislation
Infiltrating supply chains	Collecting information, crippling, causing a disruption	Contracts and procurements of critical operators.	Gaining access to protected information or information that jeopardises security via the supplier of an outsourced information system.	Identifying critical operations and chains Critical assessment of procurements and outsourcing
Corruption	Vilifying, blackmail, increasing distrust	Decision-makers, office holders, company representatives	Bribing a decision-maker or office holder and/or exposing them to create distrust.	Openness Risk management processes and assigning responsibility for monitoring

APPENDIX 2

Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

Hack for Society – Survey to members of the City Council about hybrid threats

1. What do you think about the statement: Helsinki's local policy has significant foreign policy impacts?
Answer choices:
I strongly agree / I partly agree / I neither agree nor disagree / I partly disagree / I strongly disagree

2. What do you think about the statement: Foreign policy has significant impacts on Helsinki's local policy?
Answer choices:
I strongly agree / I partly agree / I neither agree nor disagree / I partly disagree / I strongly disagree

3. How would you describe the interrelation between foreign policy and Helsinki's local policy?
Please answer in your own words.

4. What are the most significant threats against Helsinki now or in near future?
Looking ahead, what possible threats against Helsinki can you see?
Please give 1-3 answers, beginning with the most important.

5. What actors do you feel are the biggest threats against Finland?
Who or which actors may be trying to influence Finland negatively or harm the country?
Please give 1-3 answers, beginning with the most important.

6. What actors do you feel are the biggest threats against Helsinki?
Who or which actors may be trying to influence Helsinki negatively or harm the city?
Please give 1-3 answers, beginning with the most important.

7. What are the actors you mentioned trying to achieve regarding Helsinki?
What goals or objectives do the actors you mention have concerning Helsinki?
Please answer in your own words.

8. How exposed do you think Helsinki is to the following threats?
Answer choices:
1 Not at all – 2 Slightly exposed – 3 Rather exposed – 4 Significantly exposed – 5 Strongly exposed
– Economic pressures
– Corruption
– General attitudes being influenced
– Terrorism
– Conflict between population groups.
– Critical infrastructure being weakened or knocked out
– Cyber attack or disturbance
– Information manipulation on the Internet (e.g. false/fake news)

9. Can you think of other threats against Helsinki?
Please answer in your own words.

10. Do you feel that safety in Helsinki has become better or worse these last three years?
Answer choices:
Become clearly better / Slightly better / No difference / Become slightly worse / Clearly worse / Hard to tell

11. How do you feel about your own knowledge and skills in safety matters?
Answer choices:
Good / Pretty good / Rather poor / Poor

12. Please feel free to mention other possible threats against Helsinki that you can think of, or to add to your views, or give comments to the makers of the survey.
Please answer in your own words.

The role of cities as targets of various hybrid threats is significant and growing – if for nothing else, because of global urbanisation. In the present decade, population growth has been exceptionally rapid in Helsinki. A great deal of the decisions influencing people's everyday lives are made by cities' boards and councils. The functions that cities are responsible for provide channels for influencing while, also, playing a key role in responding to various hybrid threats. Aware of this, the City of Helsinki has commissioned this report. The purpose of the report is to provide basic knowledge of hybrid influencing and to promote better understanding of the subject.

Helsinki