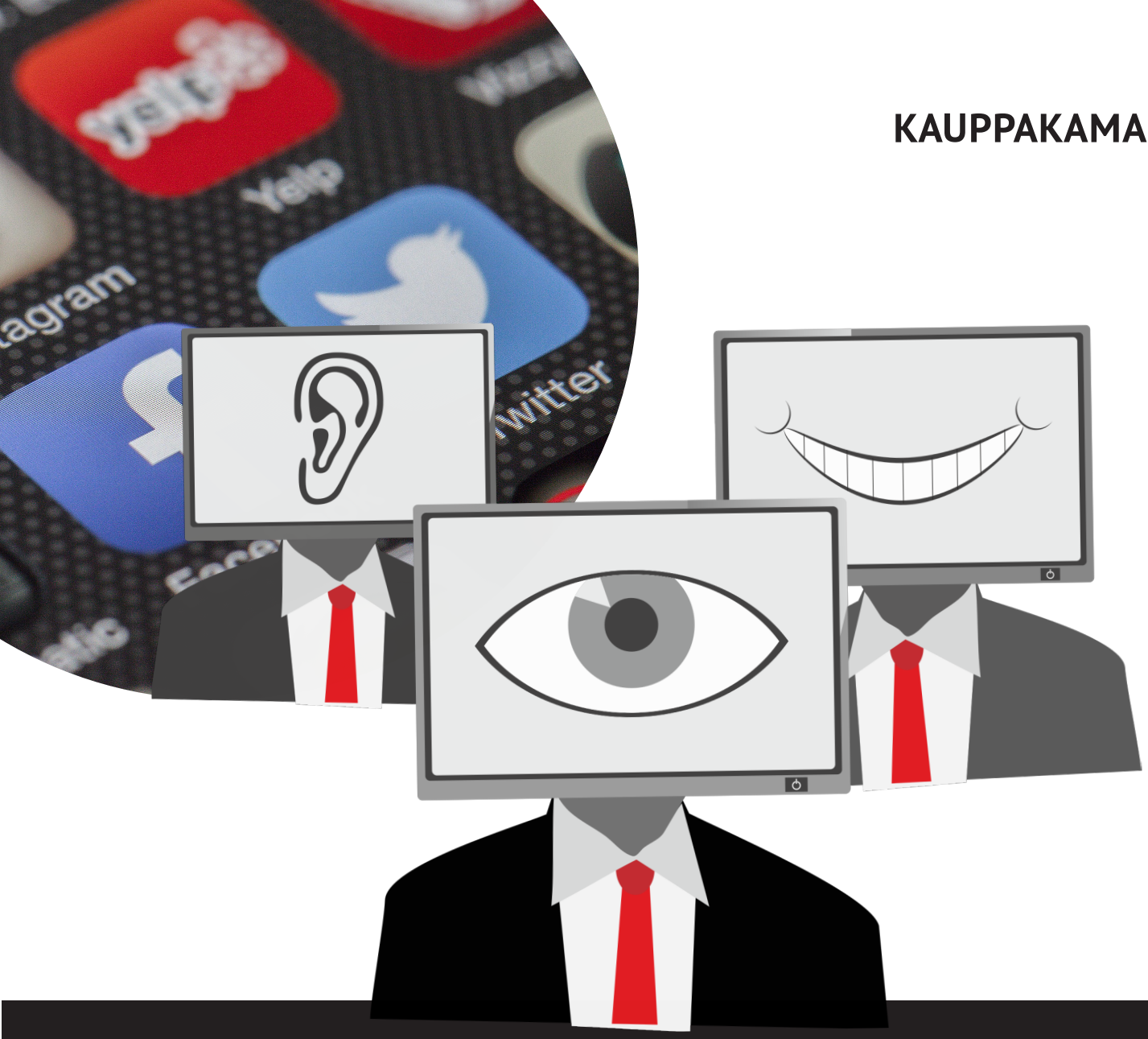
KAUPPAKAMARI



Business community and hybrid threats

2018

June 2018

Helsinki Region Chamber of Commerce,
Kalevankatu 12, FI-00100 Helsinki
www.helsinki.chamber.fi

Panu Vesterinen, Helsinki Region Chamber of Commerce, **Chris Fogle**, CyVantage Llc,
Pasi Eronen Foundation for Defense of Democracies

CONTENT

1 INTRODUCTION 4
2 COMPANIES AS TARGETS OF HYBRID INFLUENCING 6
Possible reasons for targeting a company with hybrid activity 6
Company weaknesses utilised by foreign actors attempting to exercise influence 7
The probability of being targeted with influencing activity by criminal or foreign state actors 8
Access of criminals or foreign intelligence services to company information 8
3 HOW THE COMPANIES PREPARE FOR HYBRID INFLUENCING 10
Guidelines or operating models in case of risks 10
Information resources relating to hybrid activity/actors 11
4 CONSEQUENCES OF CRIMINAL ACTIVITY AND HYBRID INFLUENCING 12
The most serious consequences of hybrid influencing 12
Have you detected any activity targeting your own business or somebody else's business that could constitute a hybrid operation or part thereof? 13
5 EXPECTATIONS REGARDING AUTHORITY INVOLVEMENT IN HYBRID THREATS AND COOPERATION 14
Should the Finnish authorities support the business community by, for example, preparing guides related to hybrid threats and organising training and exercises? 14
Does the company share information with the Finnish safety authorities when it detects suspicious activity targeting the company either abroad or here in Finland? 14
6 THE COMPANIES' ABILITY TO WITHSTAND DISRUPTIONS TO THE AVAILABILITY OF RESOURCES 16
Withstanding the loss of the following items 16
Electricity 16
Internet 17
Information systems 18
7 CONCLUSIONS 19

1 INTRODUCTION

The aim of the Business Community and Hybrid Threats report was to study how the business community and its companies here in Finland see and understand hybrid threats; what kind of phenomena are hybrid threats and hybrid influencing; how are companies targeted with hybrid threats and activity, and how are the local companies preparing against such threats.

Hybrid threats and influencing is a wide and continuously evolving concept. The influencing activity can target, for example, political decision-making, activities conducted by the authorities, the business community and its activities or any combination of these. Hybrid activity takes advantage of the vulnerabilities identified in its targets, whether they are individuals, organisations or society as a whole. Fundamentally, hybrid threats and hybrid influencing are usually carried out as state-level power games in which the states use both traditional and atypical instruments of power in a carefully orchestrated manner to reach their goals. They aim to do this without breaching the threshold of detection or, in more severe cases, the threshold of traditional, and often costly, war.

It is particularly challenging to define hybrid threats in more detail because the hybrid actors behind the influencing activities engage in their actions using old, well-known tactics. They also have access to new tools and methods never utilised before – that were never even thought to be possible to be used as weapons in support of a political agenda. These activities include old tricks, such as bribing or coercing individuals into cooperation, but also new tools that digitalisation has brought about across all of society. Examples of these tools are cyber espionage and attacks, penetration of critical infrastructure as well as information operations using social media.

It may often be hard to attribute these activities to a certain country or organisation since the activities are often conducted by a proxy operator such as a third state, front organisation or shell company, organised crime or an individual operator. At times, political or economic realities may prohibit the targets from reporting the attacks or attributing them to a certain perpetrator.

The nature of hybrid operations usually falls within the realms of classic diplomacy, information operations, military threats and economic influence. In practice, hybrid influence operations are manifested in gaining political influence, launching disinformation campaigns, stealing and leaking confidential information, conducting airspace incursions and other aggressive military manoeuvres as well as pressing economic sanctions, fuelling corruption and luring others in by politically motivated economic cooperation.

As its name suggests, hybrid influencing combines more than one form of exercising influence in support of achieving the perpetrator's political goal. This combination of activities does not necessarily happen at the same time in a concurrent fashion. The activities can be sequenced like in the case of electoral meddling: the cyber penetration of the target system is followed by leaking the materials, sometimes even fabricated ones, which are deemed to cause the most damage. Sometimes these activities can occur over a longer period of time, from years to even decades. The activities may be dispersed both geographically and organisationally, which makes it hard for the victims and authorities to connect the dots and identify an ongoing hybrid operation or campaign.

It is noteworthy that hybrid activities are not necessarily destructive or make their targets feel threatened in the short term; sometimes hybrid influencing occurs in the form of preferential treatment or through offering a great deal. Nevertheless, this serves the bigger strategic goals of the hybrid actor. Moreover, it may be true that smaller, tight-knit societies like Finland constitute a more difficult target for hybrid influencing due to the tight societal networks and the role of reciprocal trust in them. However, once these are

breached, the hybrid actor may gain extensive and comprehensive access to the targets of their influence activities.

The business community and its companies are an inseparable part of the society and, therefore, targets of hybrid influencing as well. The role of the business community has grown over the past decades as companies have increasingly assumed ownership of the services and started running them in sectors such as telecommunications, media and energy. Previously, these were delivered either by local municipalities, regional authorities or the state. Typically, the companies also continue to take care of these critical services and infrastructure both in normal situations and cases of crisis. Moreover, the public sector and authorities are increasingly dependent on technologies, resources and services provided by companies in the private sector to support their core functions and mission.

While an individual company may not necessarily be the final or even the key target of an operation, it can be instrumental in reaching the final strategic goal, such as gaining long-term access to decision-makers or their networks. In an ongoing hybrid operation, one company may be subjected to a cyber-attack, another one to an information operation, a third one to a hostile takeover and a fourth one to a classic break-in. None of the targets have visibility into the whole operation. Since hybrid influencing requires an understanding of the targets' vulnerabilities to succeed, the operations are typically preceded by information collection efforts over a long period of time. The following methods can be used: infiltration of the target organisation; utilising traditional human intelligence methods; penetrating the target's information systems by the means of a cyber-attack, or a combination of these.

The business community in general, and the companies in particular, play an important role in hybrid influencing activity. Because of this, it is important to build proper corporate security functions in the companies, raise awareness among the owners, leadership and employees, and exchange security-related information between companies and within the supply and value chains. Moreover, cooperation with the authorities provides a platform for the companies to counter hybrid threats. Examples of such cooperation include exchanging information with the authorities; participating in training initiatives conducted by the authorities, ensuring preparedness on a national level; and engaging in exercises related to building and testing capabilities for countering hybrid threats locally and nationally.

The results in this report are based on the information collected from more than 700 companies in Finland which answered the questionnaire sent to them. Thus, in addition to gaining insights from the members of the business community, this final report and its precedent also serve the purpose of increasing the awareness of hybrid threats among the members of the Finnish business community.

This report is a part of Helsinki Region Chamber of Commerce's activities that enhance corporate security. Helsinki Region Chamber of Commerce has more than 7,000 member companies representing all business sectors. Chambers of commerce in Finland have more than 20,000 member companies in total.

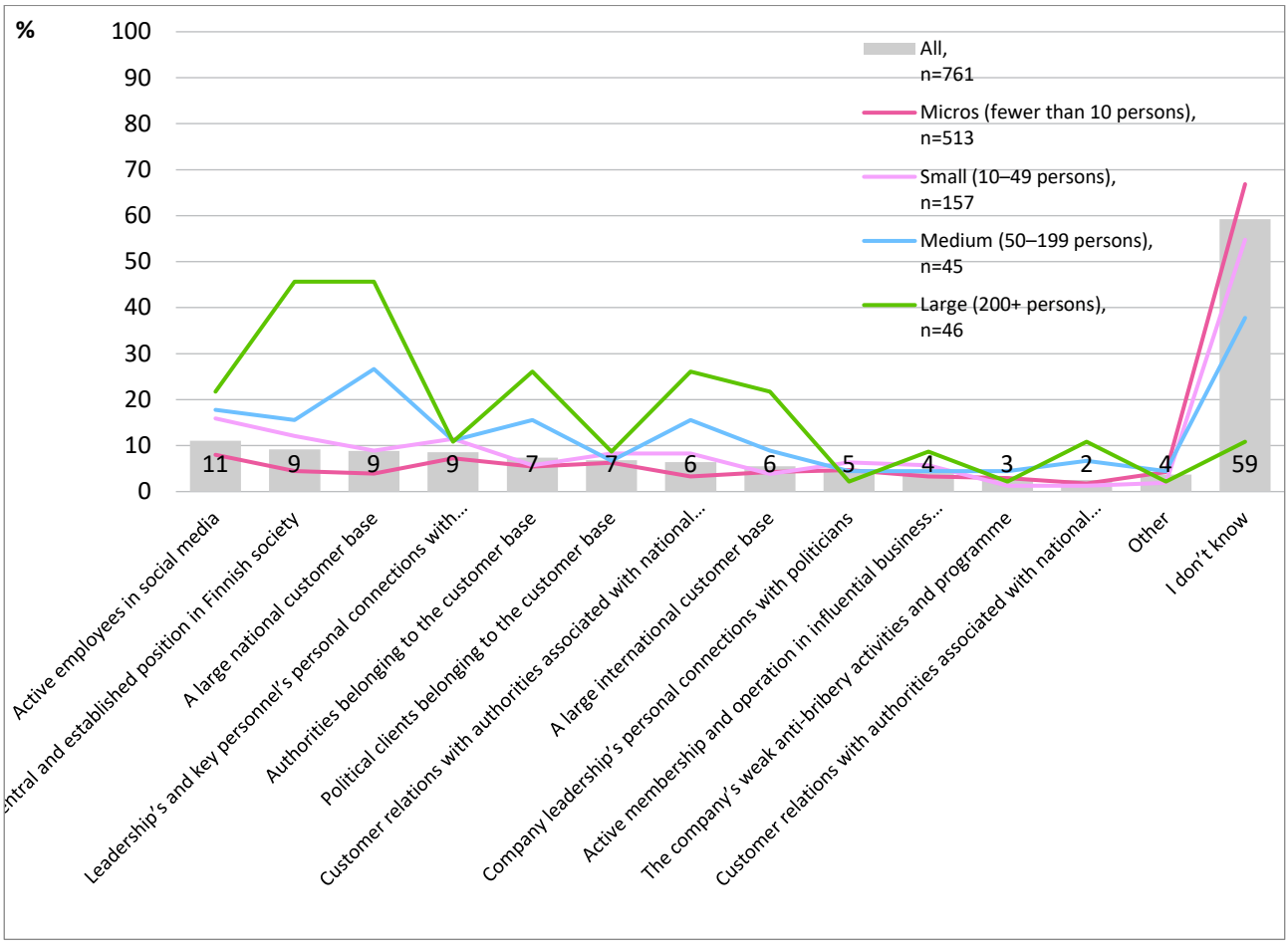
2 COMPANIES AS TARGETS OF HYBRID INFLUENCING

Possible reasons for targeting a company with hybrid activity

More than a half of the companies (59%) were unable to give reasons as to why they could be targeted with activity whose ultimate objective would be to influence the population or government in Finland or some other country. The response indicates that the subject is difficult to identify and that the business community has not yet understood its own role as a target of hybrid influencing.

The most common reason (11%) given were company employees active in social media with many followers. There has been much public debate about electoral intervention in different countries. In this respect, other types of influencing activity have been almost completely eclipsed by influencing through social media. Companies cannot yet identify all the reasons which could set them up as targets of hybrid activity.

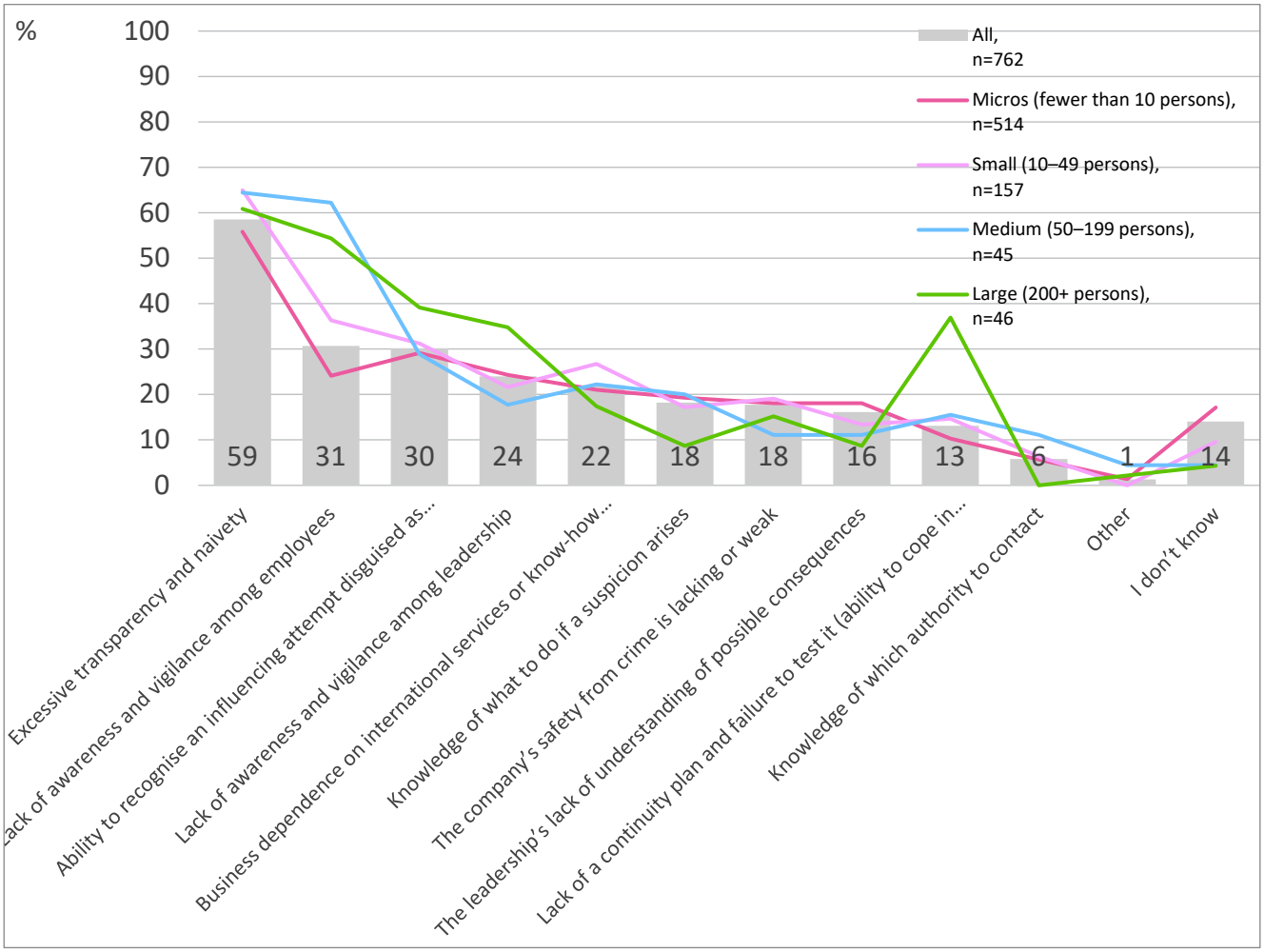
When considering why a company could become a partial target of a hybrid operation, we have to remember that this kind of activity is often conducted between states. In this type of activity, several actors can be utilised, such as foreign or local professional criminals, operators unknowingly acting as fronts, representatives of organisations as well as other operators. How the company is approached and taken advantage of depends on the ultimate objective, the target, the company's weaknesses and other factors unknown to all but those planning and conducting the hybrid operation.



Company weaknesses utilised by foreign actors attempting to exercise influence

In terms of foreign actors' (criminals or states) attempts to influence business, three major weaknesses have been identified in Finnish companies: excessive transparency and naivety (59%), a lack of awareness and vigilance among employees (31%) as well as the ability to recognise an influencing attempt disguised as business activity or an initiative aiming to take advantage of a company in an attempt to influence the actual target (30%).

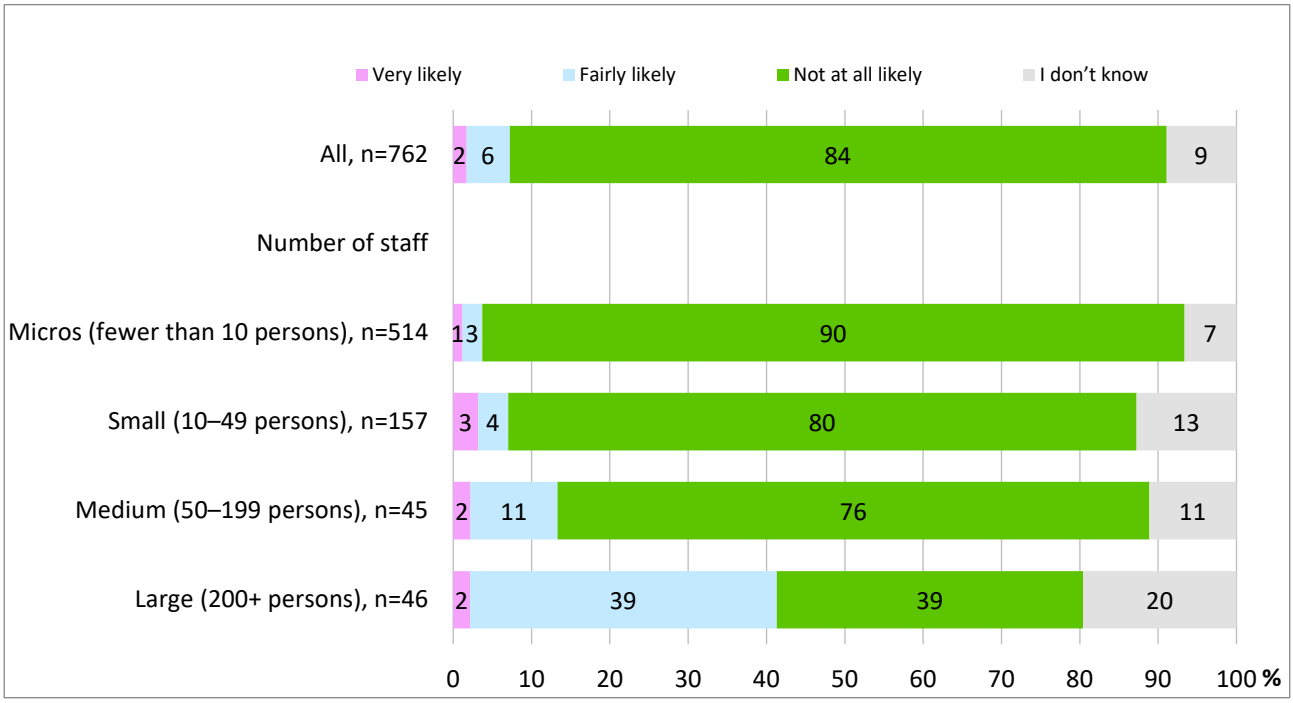
There is not enough information available about hybrid influencing and espionage. Transparency, naivety, lack of awareness and vigilance or the ability to recognise issues are matters that can, more or less, be corrected by sharing information and providing training to the extent that such corrections are possible. A hybrid actor may place surprisingly great importance on utilising people besides information and cyber influencing activities – specifically because Finland is a widely networked and small society.



The probability of being targeted with influencing activity by criminal or foreign state actors

One out of ten respondents (8%) considered it is at least fairly likely that they could be targeted with hybrid activity by criminal or foreign actors. In practice, the number of companies that could be considered interesting targets in terms of hybrid influencing or illegal surveillance is higher. It is difficult to recognise hybrid influencing efforts, and many companies are not even aware of being potential targets. Because of this, there is a particular need for the authorities to provide training and distribute information.

Of large companies (200+ persons), 41% estimated that the probability of being targeted with hybrid influencing is fairly high. Large companies are prominent, and they often have a large customer base, governmental clients, relations with politicians, commissions relating to society infrastructure as well as other factors which may set them up as targets in hybrid operations. Of medium-sized companies, more than a tenth (13%) believed that this is at least fairly likely.

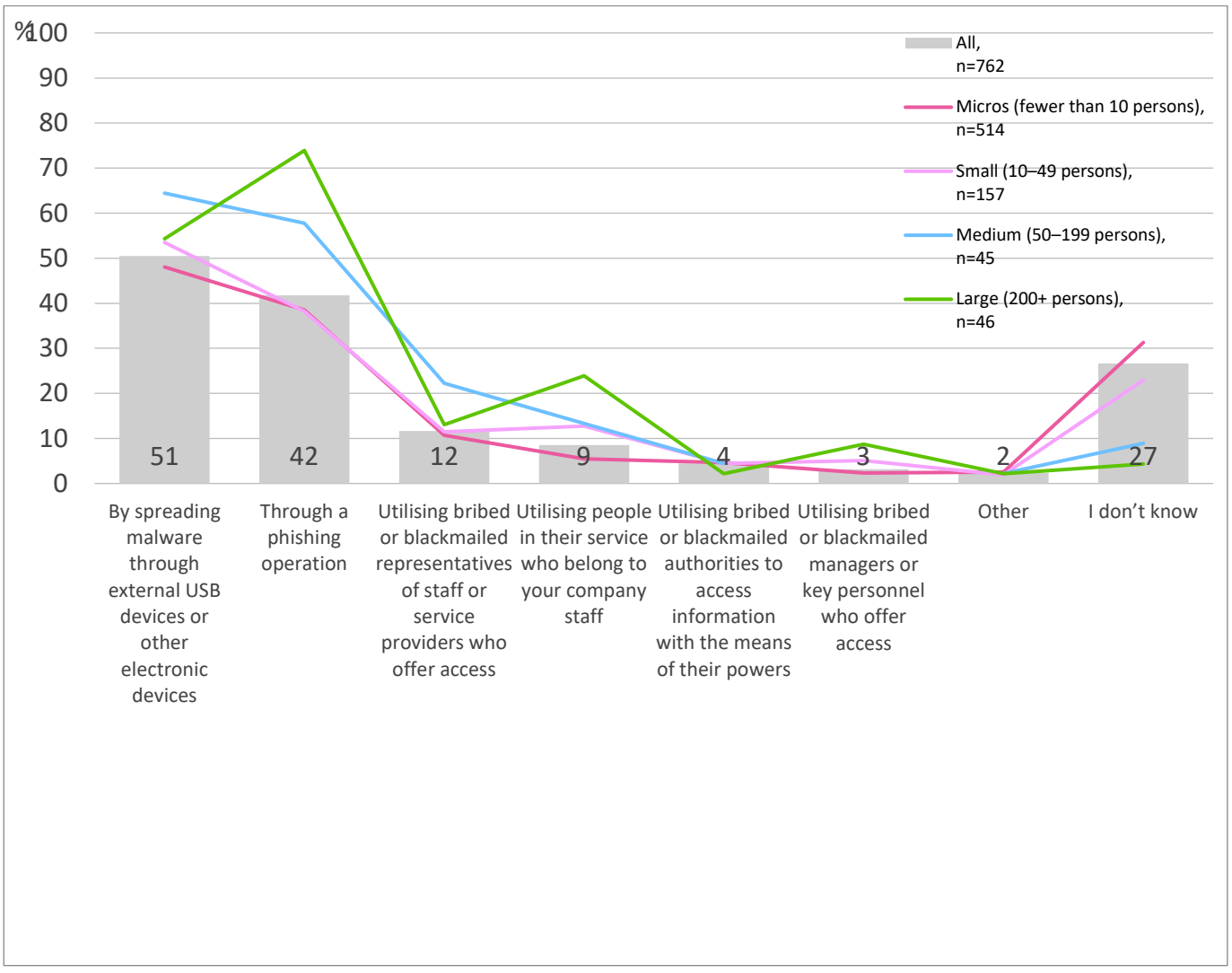


Access of criminals or foreign intelligence services to company information

Criminals or foreign intelligence services are believed to be able to access the information of their chosen company by spreading malware through external USB devices or other electronic devices (51%) and through phishing operations (42%).

The former are surely the most common means to access the information of the targeted companies via information systems. Information acquired in such a manner can be used to influence people. The information being utilised may seem harmless enough: who is responsible for which accounts, who attends the same social clubs as a political decision-maker and so forth. When a person is identified in such a manner, and when this information is connected with the person's social media profile information, behaviour on the Internet and information gathered from other sources, a professional hybrid actor may be able to form a comprehensive overview upon which they can act.

In comparison with smaller companies, large companies were more likely to mention phishing operations (74%) and using recruited people for information collection inside the target company (23%). Of all respondents, every tenth (9%) considered recruited people as the means of access to company data. Using recruits may be very fruitful: they are able to access all kinds of information based on their tasks, know where to look for specific information, and can easily find out the weaknesses of persons in positions of influence as well as what is going on in the company. This counts as information that may help a hybrid actor to judge whether it is worthwhile to target the company with a hybrid operation. Regardless of whether the company is the ultimate target or just an instrument in or a pathway to influencing the ultimate target. One benefit of utilising people is that the persons operating inside the company are able to access this information in a way that hardly leaves a trace distinguishable from normal work, or recognising these activities as such is otherwise almost impossible.

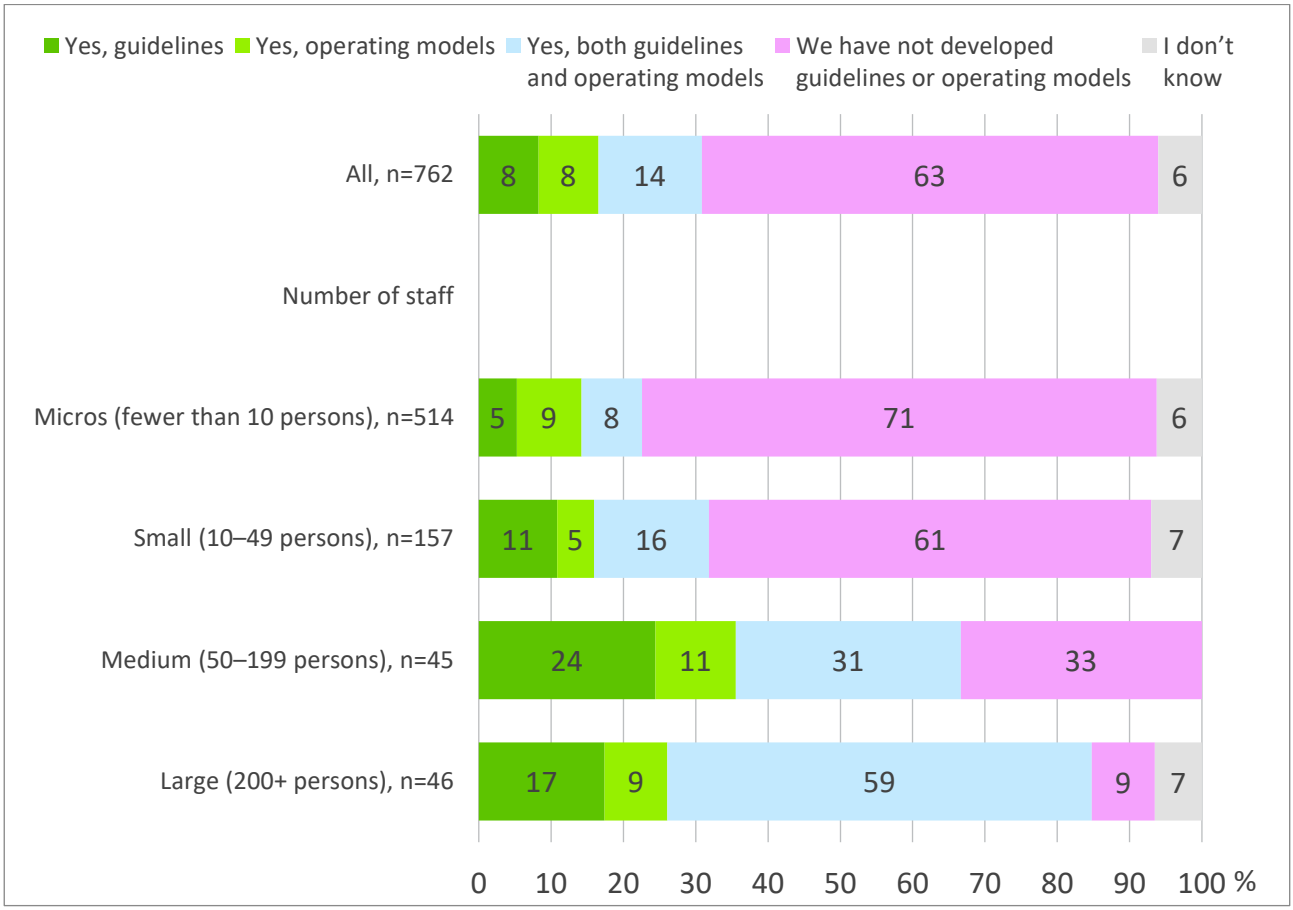


3 HOW THE COMPANIES PREPARE FOR HYBRID INFLUENCING

Guidelines or operating models in case of risks

Two thirds of the respondents (63%) have not created guidelines or operating models to protect company data in order to prevent the means of access as outlined herein. Approximately every third company (30%) has compiled guidelines, operating models or both. Companies which employ more than 50 persons, in particular, utilise either guidelines or operating models or both (66%).

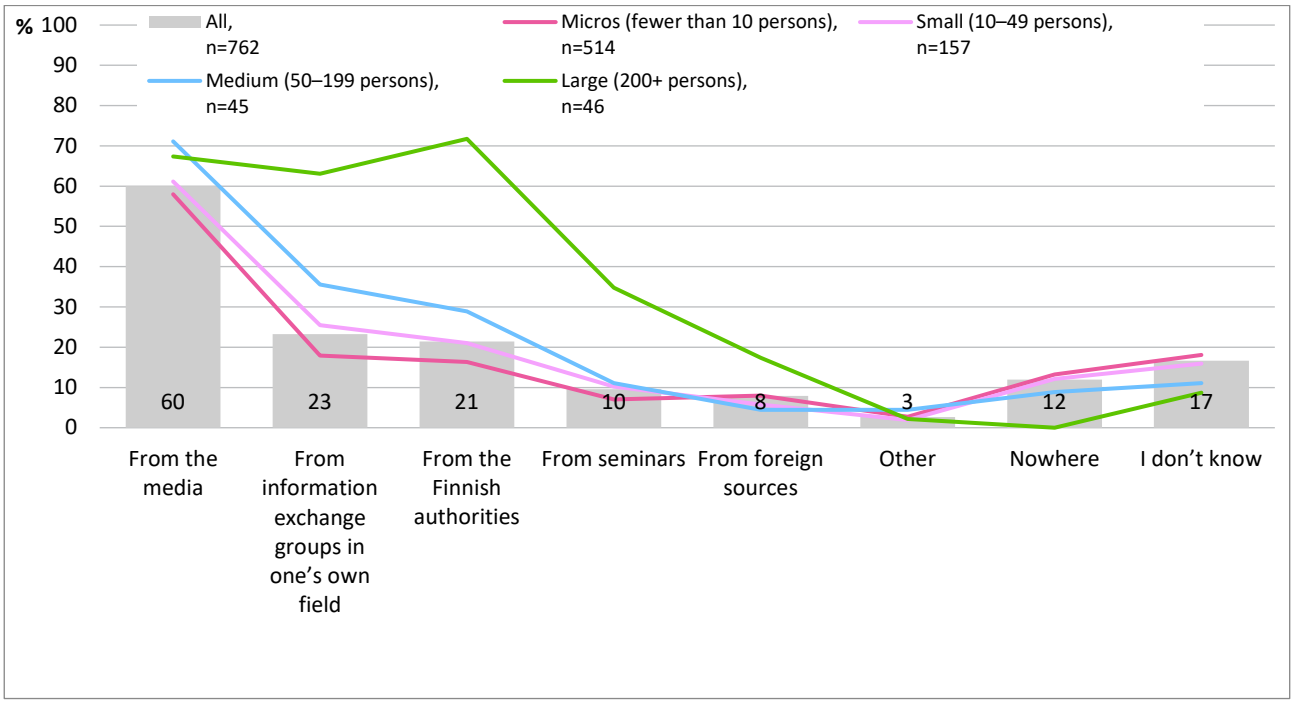
On the other hand, since there is a wide variety of criminal activities which target information and use hybrid influencing as well as a number of other means, it may not even be possible to create guidelines or operating models for all scenarios. What is crucial in these situations is the general safety-related vigilance of the employees. This vigilance can be further increased by sharing information, providing training and building a safety-positive corporate culture on a long-term basis.



Information resources relating to hybrid activity and actors

A majority of the companies (60%) obtains information related to hybrid operations, activity or actors from the media. In addition, information is acquired from information exchange groups in one's own field of operation (23%) as well as the Finnish authorities (21%). Authorities as a source of information are a major factor among large companies (72%).

All in all, it is beneficial to acquire information from multiple sources, but just like with any other information it is important to assess the validity of the sources. Because of this, it is important that the authorities assume a bigger role in producing communication and materials related to hybrid activity to the business community. The authorities could also act as natural instigators of information sharing communities and, later on, as information producers in these communities.



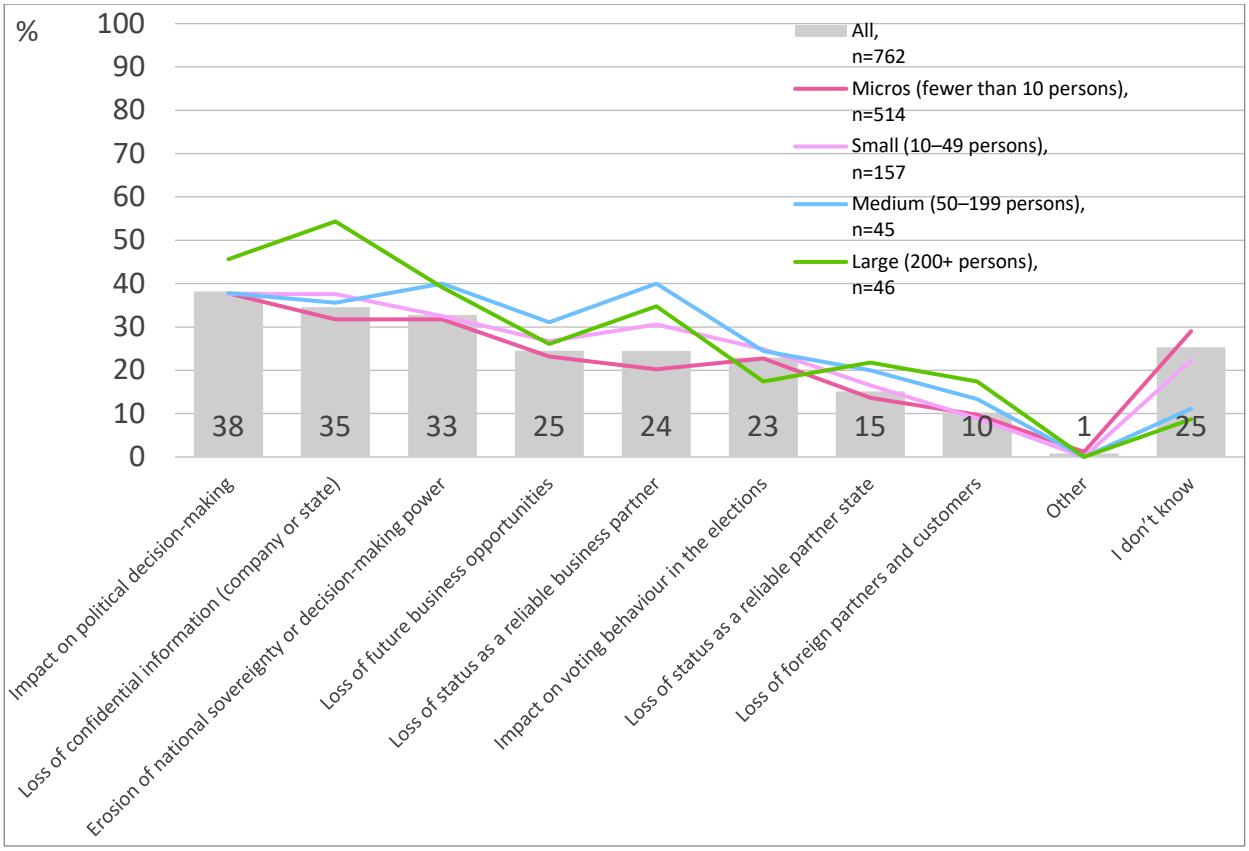
4 CONSEQUENCES OF CRIMINAL ACTIVITY AND HYBRID INFLUENCING

The most serious consequences of hybrid influencing

The three most serious consequences of hybrid influencing are the impact on political decision-making (38%), the loss of confidential information (company or state, 35%) as well as the erosion of national sovereignty or decision-making power (33%).

Traditionally, hybrid influencing has been considered an activity conducted between states and targeting states. However, if somebody wants an individual company to operate in a certain way, it is just as likely that the company is targeted in its target country. Again, the range of instruments used depends on many case-specific factors, such as the weaknesses of the company and its key personnel, the desired objective as well as the company's status in the target country and its home country. On the other hand, instead of the company's home base, hybrid activity may target the company's country of operation in case the company has a status or contacts there that the hybrid actor considers necessary.

Hybrid actors may be persons employed by a foreign state, representatives of foreign business communities or organisations, or foreign or domestic criminals. It is noteworthy that "foreign" does not simply denote citizens of the state conducting hybrid activity. The actor may be a citizen of a third country or somebody presenting as such and operating on behalf of the state conducting hybrid activity. Hybrid influencing is the sum of several activities, and there are no rules or restrictions for the means employed in this kind of activity.

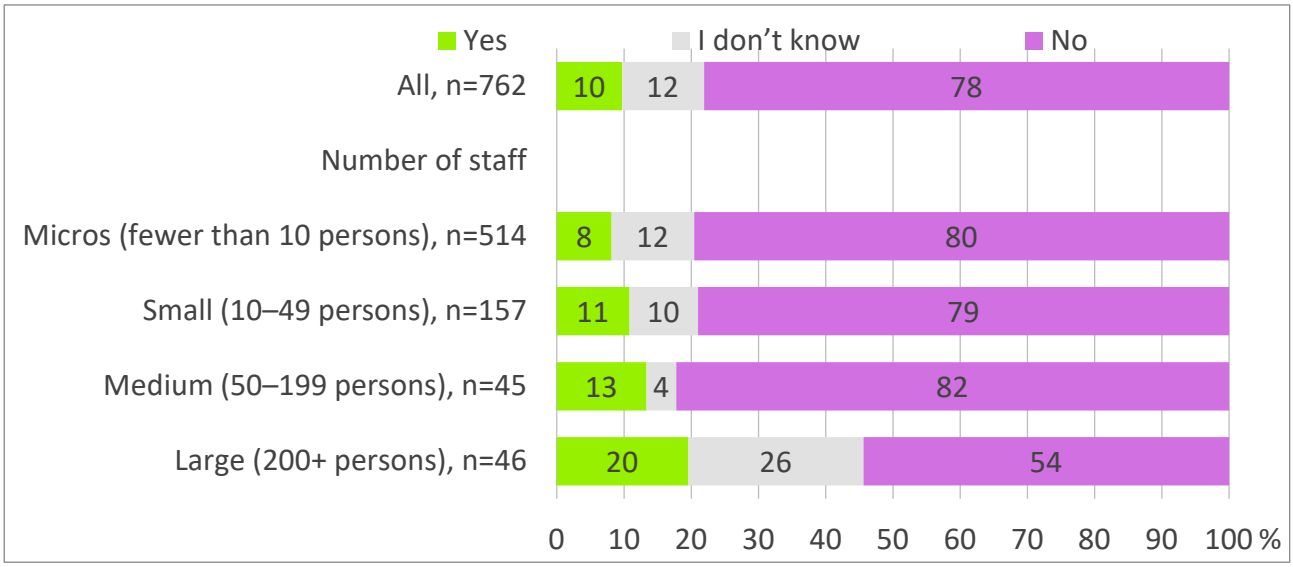


Have you detected any activity targeting your own business or somebody else's business that could constitute a hybrid operation or part thereof?

A majority of the companies (78%) have not detected any activity targeting their own business or somebody else's business that could constitute a hybrid operation or part thereof (a foreign criminal organisation or a state operating in the background). However, of all respondents, every tenth (10%) has observed such activity.

The larger the company, the more frequent such observations are. Of large enterprises, as many as every fifth (20%) has detected this type of activity. Naturally, large companies are more susceptible to hybrid operations in terms of their customer bases, contacts and status.

The fact that every fifth large company participating in this survey has experienced hybrid influencing is an indication that this type of activity, in all likelihood, is more widespread than previously thought. In their future plans, the authorities should take into account any hybrid activity targeting the business community or taking advantage of it.

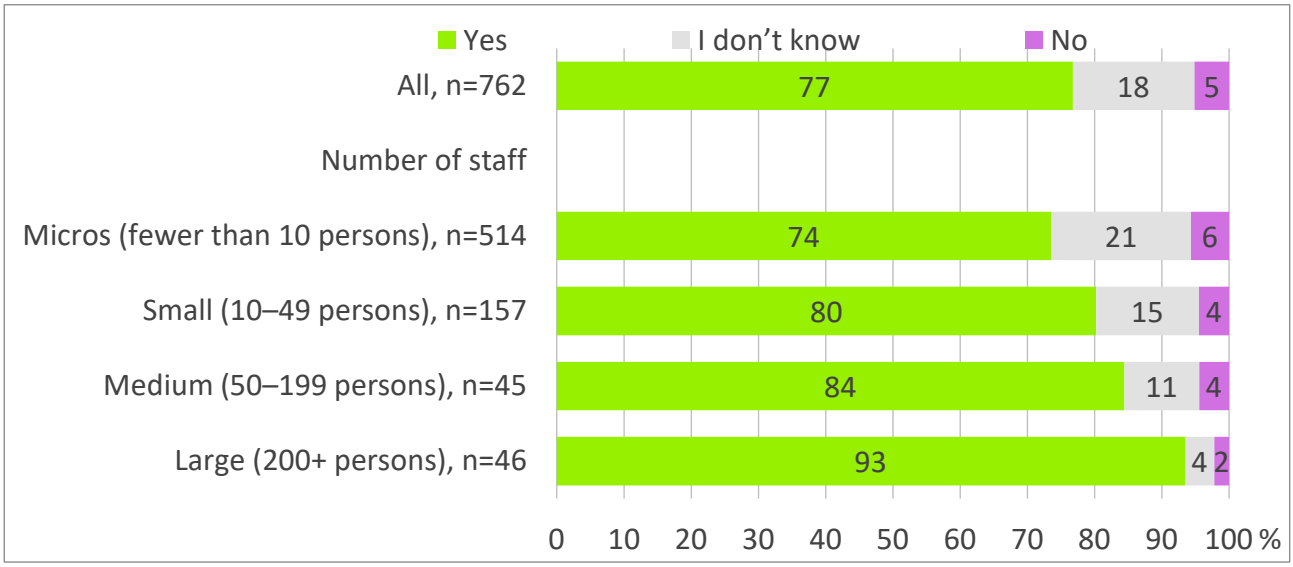


5 EXPECTATIONS REGARDING AUTHORITY INVOLVEMENT IN HYBRID THREATS AND COOPERATION

Should the Finnish authorities support the business community by, for example, preparing guides related to hybrid threats and organising training and exercises?

A majority of the companies (77%) think that the Finnish authorities should support the business community by, for example, preparing guides related to hybrid threats and organising training and exercises. Vast majority, 93% of large companies and 84% of medium-sized companies are of this opinion. The companies' need for information and training is particularly clear.

The authorities play a very important role in producing neutral and reliable material. For the business community, the best and most effective way to prepare for hybrid influencing is to acquire training and information. As a threat, hybrid influencing seems complex and irregular. Because of this, it is difficult to prepare very detailed guidelines or operating models to account for the threat. General awareness and know-how assume a central role. Whenever a threat is identified, or a suspicion arises, one must know who or what to contact. One should be able to expect smooth cooperation and activeness on the part of the authorities.



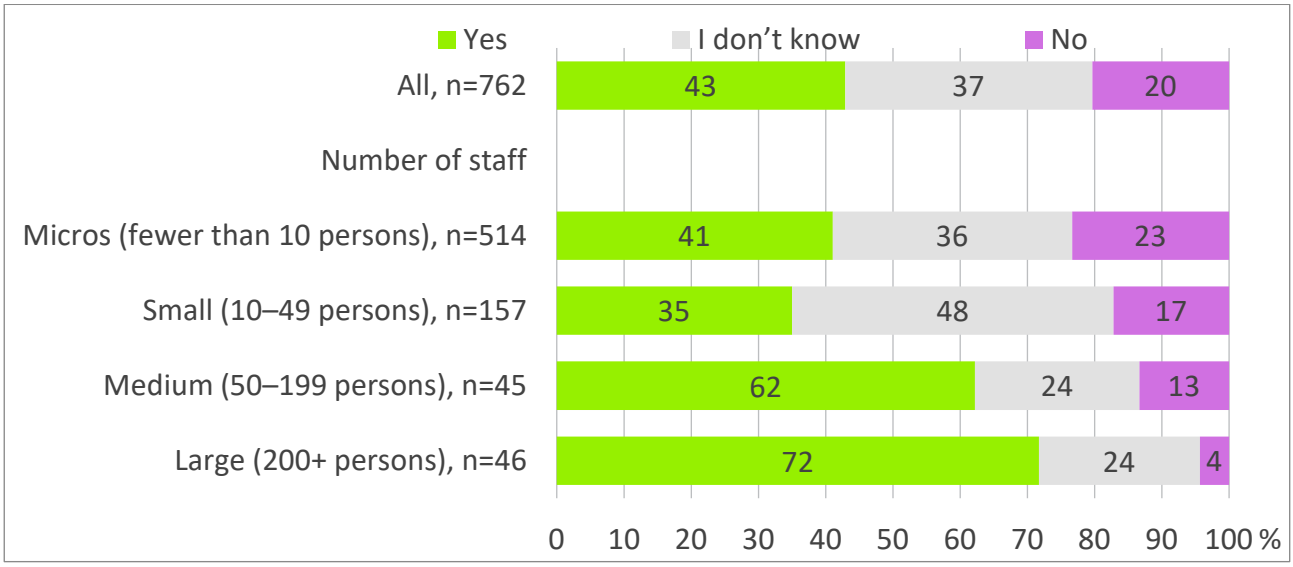
Does the company share information with the Finnish security authorities when it detects suspicious activity targeting the company either abroad or here in Finland?

Slightly less than half (43%) of the companies share information with the Finnish safety authorities on their own initiative when they detect suspicious activity targeting the company abroad or in Finland. A majority of the large companies (72%) share this information.

Being informed of suspicious activity helps the authorities to take the correct course of action. This information may help the authority to form a picture of the situation, and by analysing the information they

could gain an insight into what the hybrid actor is aiming for. Close cooperation with the business community enforces the whole society's preparation for hybrid threats.

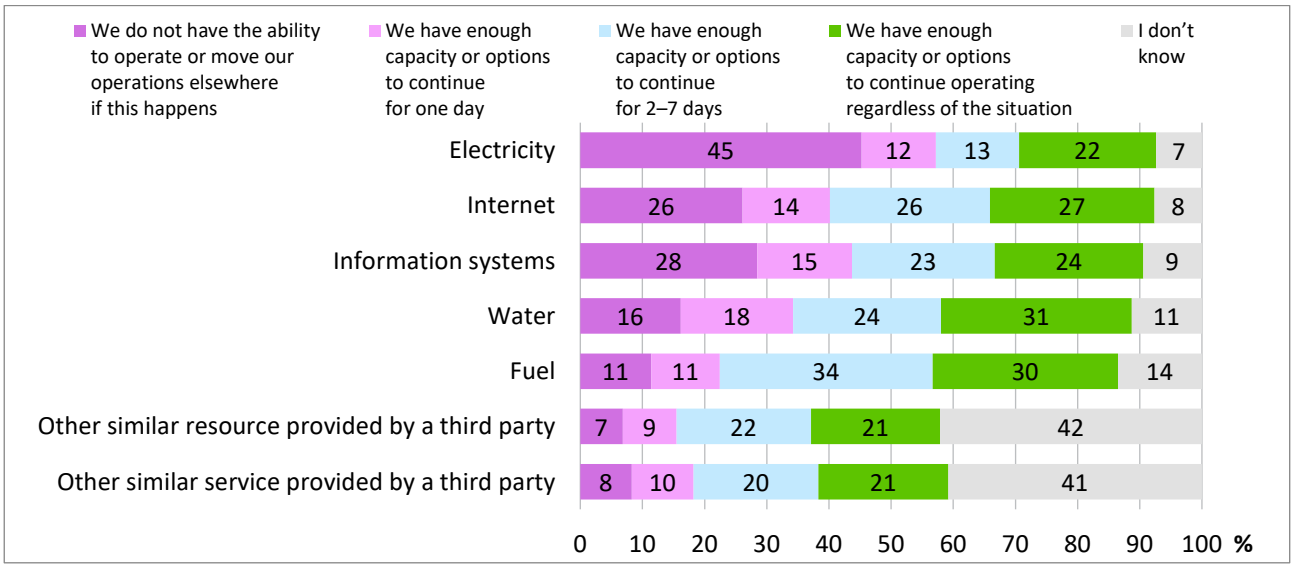
Active cooperation between the companies and authorities makes the hybrid actor's job more difficult. When a hybrid actor chooses a company as a target, it must take into account the risk that the company could give a warning of the activity. The hybrid operation as a whole might then be subjected to surveillance. In this respect, we can talk about preparation that encompasses the whole society, with the business community playing its own role.



6 THE COMPANIES' ABILITY TO WITHSTAND DISRUPTIONS TO THE AVAILABILITY OF RESOURCES

Withstanding the loss of the following items

Hybrid activity may lead to a situation where the resources and systems normally available to companies are no longer accessible to them. This kind of situation represents the other extreme of hybrid activity in which the activity is no longer disguised. This is why the company should prepare a business continuity plan which helps it to continue operating under these circumstances. Continuity plans are becoming necessary because of cyber-attacks and, occasionally, weather conditions. Situations which threaten business continuity may become more frequent in the near future.



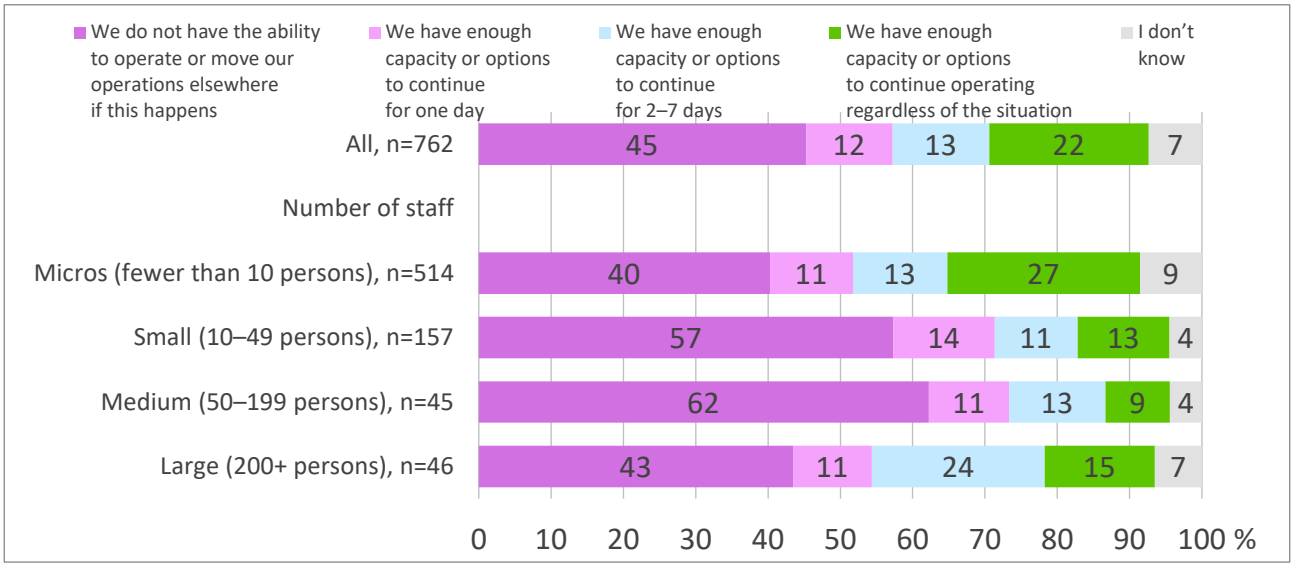
Electricity

The most critical factor in terms of a business being able to operate is the loss of electricity. Almost a half of the respondents (45%) do not have the ability to continue operating or move their operations elsewhere. Among microenterprises only (employing less than 10 persons), every fourth (27%) has enough capacity or options to continue operating regardless of the situation. This may be explained by the fact that employees in microenterprises can easily resume working remotely. Therefore, it may be easy to operate in a place where electricity is available.

A tenth (12%) of the respondents are able to manage for one day. This means that after one day, almost two thirds (57%) of the companies are unable to continue operating. Even with large companies, more than a half (54%) are unable to continue operating at this point.

Different sectors would be able to cope with disruptions in electricity distribution as follows:

Industry: 61%/not at all, and 8%/one day
Construction: 52%/not at all, and 15%/one day
Commerce: 43%/not at all, and 10%/one day
Service: 40%/not at all, and 13%/one day



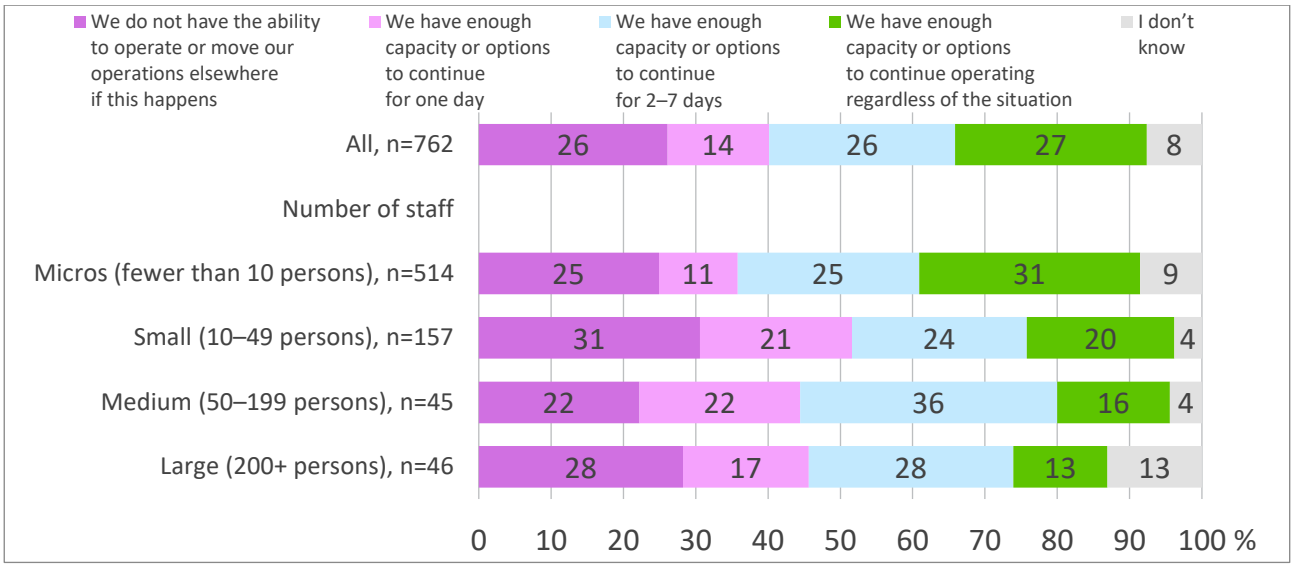
Internet

Every fourth (27%) respondent is able to cope with the loss of Internet, and approximately the same number would not be able continue operating.

One in seven (14%) respondents would be able to manage for one day. This means that after one day, four out of ten (40%) companies are unable to continue operating. Even with large companies, almost a half (45%) are unable to continue operating at this point.

Different sectors would be able to cope with the lack of Internet access as follows:

Industry: 19%/not at all, and 18%/one day
Construction: 21%/not at all, and 11%/one day
Commerce: 30%/not at all, and 22%/one day
Service: 28%/not at all, and 11%/one day



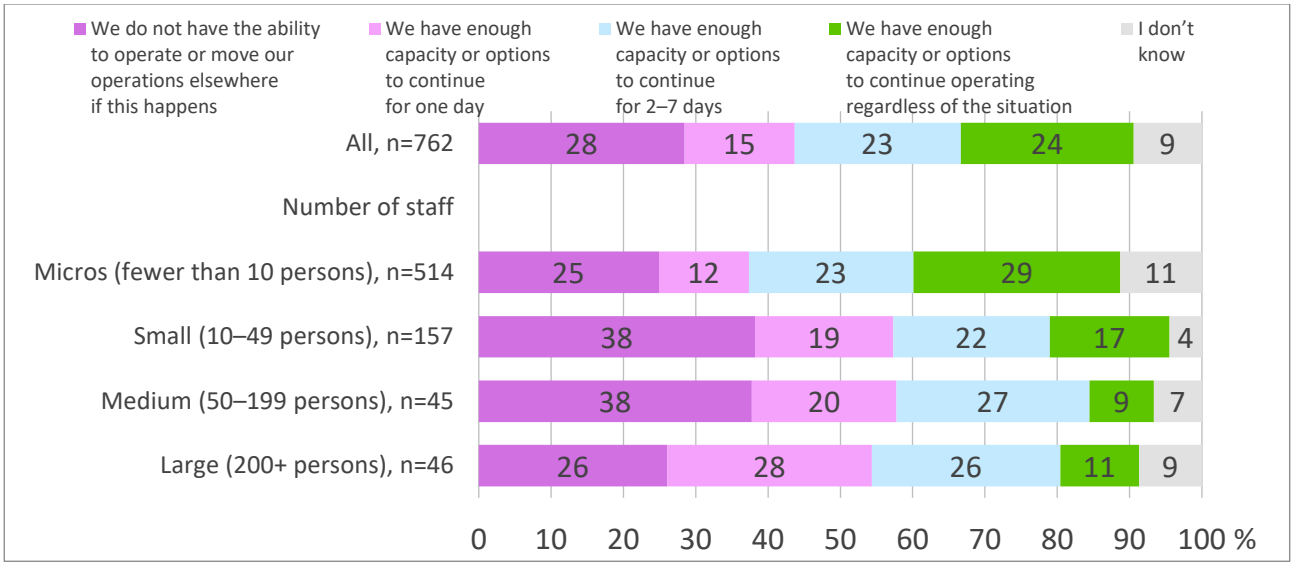
Information systems

Approximately every fourth company (24%) is able to cope with the loss of information systems. A slightly larger percentage, 28%, is completely unable to operate without them.

Approximately every sixth (15%) company is able to manage for one day. Therefore, after one day, more than four out of ten (43%) companies are unable to continue operating. Even with large companies, more than a half (54%) are unable to continue operating at this point.

Different sectors would be able to cope with the lack of access to information systems as follows:

Industry: 27%/not at all, and 21%/one day
Construction: 22%/not at all, and 11%/one day
Commerce: 30%/not at all, and 23%/one day
Service: 30%/not at all, and 13%/one day



7 CONCLUSIONS

Hybrid activity targeting the business community is already a commonplace occurrence?

Every tenth company participating in the survey recounts instances of being targeted with hybrid activity. Hybrid activity occurs most commonly among large companies; every fifth has been targeted with this type of activity. There is a considerable amount of activity targeting companies that can be classified as hybrid influencing. This highlights the need to expand and deepen cooperation between the business community and the authorities and to provide more resources as well.

Large companies as targets of hybrid actors

Four out of ten (41%) large companies think that it is at least fairly likely that they could become targets of hybrid influencing efforts by criminals or foreign actors.

Intelligence services and criminals are able to access company data via the Internet and by phishing – large companies are worried about an internal threat

The companies believe that the most common means (51%) is infiltration via USB devices or other electronic devices. Phishing (42%) is the second most common method. Every fourth (25%) large company is worried about their employees recruited by a hybrid actor. Access to the information exposes the companies to data manipulation and sabotage of operations as well. Hybrid actors have several ways to access company information, and they have a head start which the companies should catch up with.

The business community is worried about political decision-making and the erosion of decision-making power

The impact on political decision-making (38%) and the loss of national sovereignty or decision-making power (33%) are considered some of the most serious consequences of hybrid influencing. The companies are very well aware of the connection between hybrid influencing and national security.

Transparency and naivety open the doors to hybrid actors

Almost two thirds (59%) of the companies believe that excessive transparency and naivety, traditionally part of the Finnish culture, are the biggest vulnerabilities with regard to hybrid activity. Finland is a small and networked society, which is why this vulnerability can be considered a significant one. An effective way to fix this issue is to provide information and training.

A significant number of companies share information with the authorities and hope to have their support

The business community is prepared to share information with the authorities. Four out of ten (43%) respondents share information with the Finnish security authorities when they detect suspicious activities targeting their company abroad or in Finland. Of large companies, more than two thirds (72%) do so. A majority of the companies (77%) hope to receive guidelines prepared by and training organised by the authorities to support them in their preparation for hybrid threats.

The business community is vulnerable to disruptions in the availability of resources

The continuity of business operations is very vulnerable to disruptions in the availability of resources. A power failure lasting an entire day cuts off almost two thirds of the companies (57%), the loss of Internet access for a day stops more than a third (38%), and the inability to access information systems for a day cuts off more than four out of ten companies (43%).

KAUPPAKAMARI

Helsinki Region Chamber of Commerce
Kalevankatu 12, FI-00100 Helsinki
etunimi.sukunimi@chamber.fi
www.helsinki.chamber.fi