Cyberwatch Finland

WEEKLY REVIEW

14/2024

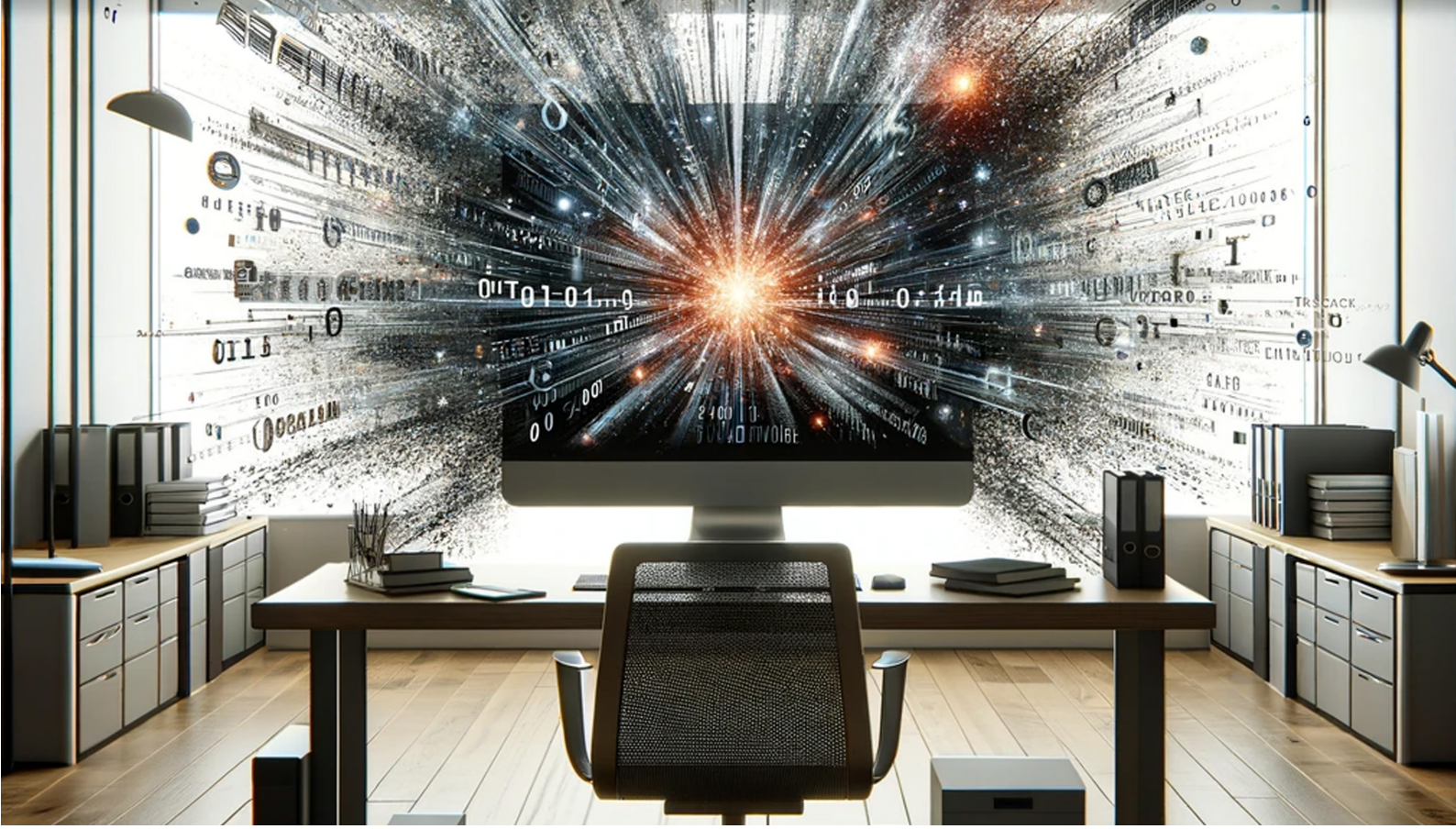
THEME REVIEW

INFORMATION WARFARE

Cybersecurity is Built by Small Actions and Management of Large Concepts

CONTENT

14/2024



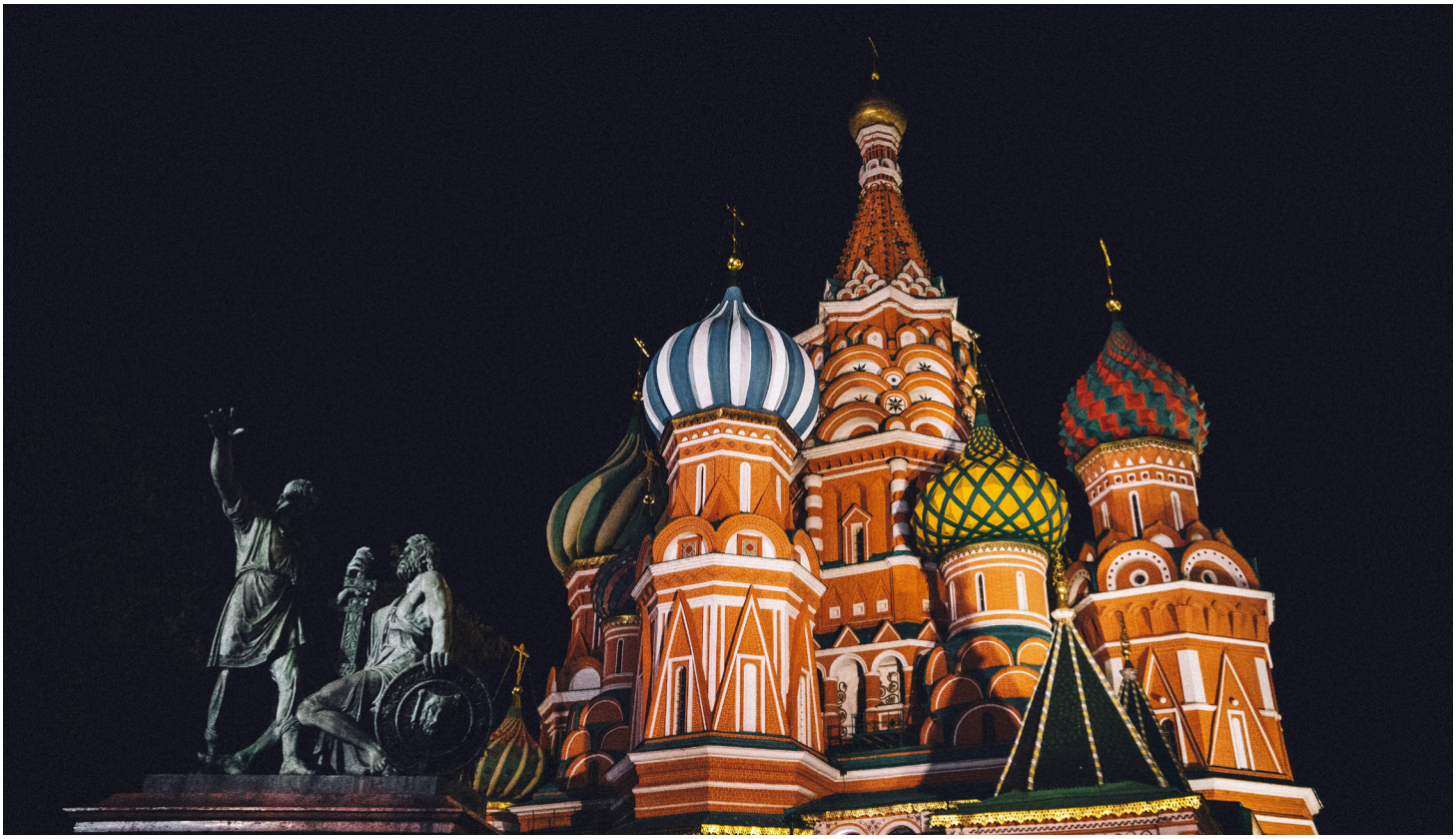
INFORMATION WARFARE IS TOPICAL. OVERVIEW OF KEY ACTORS

Information influencing is one of the oldest ways in the world to try to shape one's own operating environment or other people's perceptions to suit oneself. Different kind of information influencing and under a different name has been practiced in practice throughout human history. However, its importance has increased with digitalization, as the amount of information available or manipulable has grown exponentially. Influencing is carried out by many different actors, but typically the focus is on the most influential one, i.e. governmental information influencing. The struggle to control information or access to it is constant and intensifies during crises or politically sensitive periods. In recent years, this has seen significant growth. The struggle between states over narratives is also often referred to as information warfare. 2024 will also be an important election year in numerous countries. It is clear that increasing information influencing is also associated with these decisive moments.

Information warfare or information influencing are not easy to define unambiguously. Communication is always about influencing, and even state actors at least try to communicate strategically and shape publicity to their advantage. Likewise, false and misinformation has been spread throughout history. Defining the truth can also be challenging. It is also worth asking whose responsibility it actually is to determine the truth in the end.

In Finnish-language discussion, the terms information warfare and information influencing have been used interchangeably. However, there have been attempts to define the term. For example, according to the Security Committee, a cooperation body operating in connection with the Ministry of Defence, information influencing refers to activities in which the perceptions or actions of a target are changed through the information and opinion environment by producing, modifying or restricting its availability. Information warfare, on the other hand, is hostile influencing towards decision-making, operational capacity and opinions of the chosen target through the information environment, as well as protection against similar attempts of influencing. Other definitions have also appeared. In English-language research and articles, the distinction between information warfare and information influencing has hardly been made – the general term "information warfare" has been used to describe all kinds of activities. In Russia, when talking about information security and information warfare, a division has been used into information technological and information psychological activities. The latter is closest to the Western understanding of information warfare.

Although it may not be possible to find an unambiguous definition, it is important to examine the objectives, strategies and means of influencing the information of the most significant state actors in order to understand the phenomenon. Protection against information influencing is part of the overall resilience of societies, i.e. crisis resilience. For organisations, the identification of information influencing becomes topical in communication strategies and situations where fake news or other content that may concern their own organisation spreads.



RUSSIA – SUCCESSFUL OR UNSUCCESSFUL INFORMATION WARFARE?

Russia is waging an information war on several fronts. Information influencing is targeted, for example, at Western countries, Ukraine and potential sympathetic parties in China, Africa and Latin America, for example. It is also vital for Russia to control the information dimension within its own borders. The objectives and strategies of Russia's information warfare vary depending on the target, but common denominators can also be found.

In the West, quite a lot has been written and talked about Russia's information warfare and information influencing. The topic surfaced especially with the events in Ukraine in 2014, when Russian information operations were generally considered successful. Russia was seen to have succeeded in spreading its own narrative, for example, through Kremlin-funded media outlets operating in Western countries. In addition, fake news, Russian "trolls" on social media and strategic communications and confusion caused by the state leadership played into Russia's hands. This undermined the West's ability to respond to the crisis. Since then, the sharpest edge of Russia's information influence is thought to have lost. If in the past there was support and understanding for Russia's claims, Russian fake news or social media comments no longer seem credible in most cases. However, the situation is not straightforward. Although the credibility of Russia's narratives in the West has radically decreased, Russia has been able to at least partially determine what the West is talking about. This is also an important part of information influencing. In this respect, Russia is supported by other means of hybrid influencing, such as cyberattacks or and organising waves of migrants into border areas.

In connection with the war in Ukraine, the definition of the theme of discussion has been even more emphasized. Examples of this include talk of the use of nuclear weapons, various 'red lines' and the escalation of the conflict due to the supply of Western arms aid, such as the Leopard battle tanks. Political decision-makers always have to weigh up the message coming from Russia. In addition, headlines about, for example, nuclear weapons will certainly stick in the minds of citizens, and this alone can achieve the desired information effect. In Russia, there is so-called media power, i.e. the possibility to determine what is discussed in the media.

However, in the vast majority of Western articles and studies on the information dimension of the war in Ukraine, Ukraine is thought to have won the information war. Russia's goal has been to undermine Ukraine's national unity and influence Western support through the means mentioned earlier. Typical themes of Russian propaganda have included highlighting divisions within Ukraine, political corruption and questioning the morale of the troops. However, Ukraine, through its own strategic communication, has managed, at least satisfactorily, to respond and win over both the home crowd and the West. Claims of denazification of Ukraine and saving Russians from genocide, which are unsuccessful in the West, do of course gain sympathy within Russia and it ś own citizens.

In the so-called "Global South", including Latin America and Africa, there are still plenty of listeners to Russia's message. This is partly due to historical reasons, particularly the colonialism practised by European states at the time, and to the antipathy towards the West that still exists today. This starting position has given Russia an advantage which it is also using. At this time, the most important means of influencing information for Russia are the media houses RT and Sputnik, which are banned in the EU, and which act as the Kremlin's global messengers. However, here is no accurate, independent data on channel reach. Nevertheless, this is a large-scale and significant activity. For example, media houses mentioned in Latin America published more than 6300 articles about the war in Ukraine between January and August 2023. There are hundreds of millions of potential listeners, and the impact of the message is further strengthened through diplomacy, investments and other means of cooperation and trade.

In Russia's own information space, control has increased. The situation seems to be under control, as the mass media – television, radios and newspapers published in the country – are de facto completely controlled by the regime. Access to some Western websites and opposition newspapers has been blocked and social media has been brought under tighter control. Legislation has also sought to take action, as evidenced by, for example, laws on spreading "fake news" related to the military and army. According to the NGO OVD-Info, which monitors the state of human rights in Russia, hundreds of criminal investigations have been opened in the country for spreading anti-war messages, mainly based on publications on VKontakte and Telegram.

However, the information space is not a vacuum. For example, the very popular YouTube video platform still operates in the country. Independent and free journalism, for example, on Telegram channels is still present. It is also possible to prohibit restrictions with VPN applications that provide access to free Russian-language media abroad. However, obtaining independent information requires effort and also technical dexterity, which the more mature population does not necessarily have.

No major changes are expected in Russia's information influence in the future. The information dimension will remain in the toolbox, but especially in Western countries it will probably play only a role in other hybrid operations. Of course, strategic communication still aims to confuse and cause friction between different actors. War propaganda against Ukraine is also likely to remain unchanged, as will spreading one's message to potential audiences in Africa and around the world. However, In Russia's internal information environment and its management, the atmosphere is likely to tighten further. The operating logic of authoritarian states involves maintaining the position of those in power, to which all other actions are subordinate. The sanctions imposed by Western countries and the large number of dead and wounded will certainly be visible and affect the internal social climate in the long term. Although legislation has been tightened and services blocked, there is still room for tightening. Tougher penalties can be handed out, the rest of the platforms (such as the aforementioned YouTube and Telegram) can be banned. The development of artificial intelligence also enables more effective and credible influencing not only at home but also abroad.

CHINA – INFORMATION WARFARE SUPERPOWER

InChina, information influencing plays an extremely important role. China's military strategy speaks of large-scale informationised warfare, which encompasses all warfare in the digital world, from electronic warfare to the destruction of adversary's information systems by missile strikes. Traditional information influencing plays an important and recently emphasised role in this concept. Unlike many other forms of warfare, it can be conducted in time of official peace and at a low threshold globally. In Chinese mindset, the information environment of an adversary of the state is one of the most important targets to be influenced. Management of this state both determines international relations in peacetime and affects the outcome of possible conflicts.

Behind China's information operations is an attempt to influence the information environment of adversary states, increase its own influence and alleviate attitudes and prejudices against it in neutral states. China's information operations combine both mass production and subtle and carefully planned influencing. Especially the latter can be very difficult to identify. Influencing is targeted according to needs around the world, and the range of means also varies depending on the target audience and goal. The most important targets of Chinese influence have recently been Taiwan and Hong Kong in particular. Influencing both areas is continuous, far-reaching and systematic. Hong Kong, which was previously very largely autonomous and free of information environments, has already been brought under very strict Chinese control, and recently China has focused on Taiwan. According to the Swedish research institute Varietes of Democracy (v-dem), Taiwan has been the country most affected by foreign influence attempts and disinformation for a decade. These operations are ongoing, but their intensity varies according to current events and events in world politics. For example, the spike in the elections in Taiwan in January was clear, although the outcome of the elections may not have pleased China.

In addition to using disinformation and direct influence on target countries, China has also been identified as making effective use of social media to spread its own narratives. Virtually all social media platforms have easily recognizable Chinese "troll profiles" that replicate and make visible the views and views desired by the state. The number of these has increased in recent years, and Meta, for example, has announced that China, along with Russia, is clearly the most active country that seeks to influence the information environment through

social media. Chinese fake profiles operate in dozens of different languages and distribute news and articles designed to sink into the target country's audience. They also "like" and comment on each other's posts, increasing the likelihood that algorithms will make them visible to more people. In addition to fake profiles, China also uses social media in other ways to its advantage. For example, Microsoft's Threat Analysis Center (MTAC) has reported that it has detected social media influencers recruited and trained by China who produce mostly innocent content related to makeup or games, for example. From time to time, however, one can distinguish among this content the expression of opinions approved by the Chinese state without the creator making a big fuss about it. The obvious aim is to generalise and normalise these otherwise perhaps eye-catching points of view. Profiles work in several different languages, on practically all social media platforms, and they are much more difficult to identify than trolls.

One cannot talk about Chinese information influencing without mentioning that it also targets within the state's own borders. Controlling the perceptions of China's own citizens and immigrants living abroad, as well as managing its own information environment, is considered extremely important, and a lot is also invested in it, perhaps the most in the world. China has one of the best isolated information environments in the world, where prevailing opinions are tightly controlled by the state and there are virtually no counter-views. Thus, in Chinese strategic thinking, control of both one's own and the adversary's information environment is emphasized, and control of both is actively sought.

As with Russia, no significant long-term changes are expected in Chinese information influencing. Control of one's own information space will almost certainly remain, and operations abroad will continue. Momentary spikes in activity and the orientation of operations following global political focal points are still seen. The clearest factor of change is probably how well the West learns to recognise Chinese information influencing and how Western countries and their citizens know how to protect themselves from its adverse effects.

UNITED STATES – THE GOAL OF CONTROLLING THE INFORMATION ENVIRONMENT

Like other superpowers, the United States is a significant player in influencing through information, but its operations are more challenging to monitor than those of authoritarian states. The United States has traditionally been a democratic country that emphasizes individual freedom and self-direction, and its public information influencing arsenal does not include deceiving its own citizens or other Western societies. The U.S. Department of Defense has developed an Information Environment Operations Strategy for 2023 with a particular focus on influencing, monitoring and protecting against threats to the United States. The most acute threat to the United States is Russia, which is waging war in Ukraine. Russia is perceived as an aggressive and unpredictable entity. The United States sees China and its growing geostrategic and economic influence as a growing and long-term major threat. In addition to these, the permanent threat is the global imbalance sought by Iran and North Korea. In addition to the above, the strategy recognizes the threat posed by violent extremism against the United States and its allies.

The U.S. Department of Defense defines the information environment as a set of different factors, all of which influence how humans and automated technical systems process and acquire meaning from information. The United States wants to influence these factors in a positive way from its own point of view and protect them from external influence. In the American view, information warfare is the application of large-scale destructive force against information resources and systems, as well as computers and networks that support the four critical infrastructures: the power grid, communications, finance, and transportation.

Operations in the information environment can include military actions and vice versa. In the past, the U.S. military has preferred to resort to conventional weapons, and the potential of the information environment has been exploited to a limited extent. The purpose of the new strategy is to familiarise each military level with the functioning of the information environment. According to the strategy, the information environment must be utilised in a front-loaded manner. The aim is to

have a positive impact on the United States and the makers of automated systems and to shape the military's operating environment to be more favorable for the United States. In implementing this strategy, the U.S. Department of Defense intends to involve academic research, the private sector, non-profit organizations, and other actors in the information environment.

The United States is a global market leader in entertainment, technology and, for example, financial markets, so its potential for information influencing is huge globally. For example, the "American worldview" produced by the film industry is highly visible around the world, and it is conveyed to viewers regardless of language and culture. This type of influencing is called "soft power". Soft power refers to the ability to influence others by attracting and persuading, rather than by coercion or military force. It involves offering one's own values, culture and way of life to an international audience, both intentionally and unintentionally.

The United States expects the use of harmful digital information and communication technologies to increase and become automated in the coming years. It will also be more targeted, more complex and more difficult to interpret. This risks further distorting publicly available information. According to the US Information Environment Strategy, U.S. citizens are threatened by the exploitation of sensitive information, illegal use of technology, commercial spyware, and misuse of surveillance technologies, among others. In general, this type of activity is carried out by authoritarian states, but the United States also considers that some democracies have adopted these practices. This is contributing to the backsliding of democracy. According to its current understanding, the United States intends to address these through regulation and diplomacy as well as, if necessary, through pressure and sanctions. With this strategy, the United States is likely to invest significantly more in managing the information environment both within and outside its own borders. This means a concrete reallocation of resources and, for example, training the army to meet the requirements of the information environment.

REFERENCES:

https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/in-latin-america-russias-ambassadors-and-state-media-tailor-anti-ukraine-content-to-the-local-context/

https://www.atlanticcouncil.org/in-depth-research-reports/report/undermining-ukraine-how-russia-widened-its-global-information-war-in-2023/

https://politiikasta.fi/politiikasta-fi-raati-infosota-ja-kansallinen-narratiivi/

https://en.ovdinfo.org/persecution-anti-war-movement-report-two-years-russias-full-scale-invasion-ukraine#1

https://en.ovdinfo.org/data-politically-motivated-criminal-prosecutions-russia

https://irp.fas.org/eprint/snyder/infowarfare.htm

https://jyx.jyu.fi/bitstream/handle/123456789/81732/URN%3aNBN%3afi%3ajyu-202206153342.pdf?sequence=1&isAllowed=y

https://www.spsnavalforces.com/story/?id=802&h=Chinas-Strategy-of-Informationised-and-Intelligent-Warfare

http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html

https://www.mandiant.com/resources/blog/pro-prc-influence-campaign-expands-dozens-social-media-platforms-websites-and-forum

https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-109/jfq-109_63-73_Chin-et-al.pdf?ver=W3dp3IBzJS-u-8WyPZe-deA%3D%3D

https://www.npr.org/2023/08/29/1196117574/meta-says-chinese-russian-influence-operations-are-among-the-biggest-its-taken-d

https://www.forbes.com/sites/jillgoldenziel/2023/11/30/5-things-to-know-about-the-pentagons-information-strategy/

https://ulkopolitiikka.fi/lehti/3-2014/venaja-oppi-kaymaan-informaatiosotaa/

https://www.nytimes.com/interactive/2020/09/04/world/asia/hong-kong-speech.html

https://foreignpolicy.com/2022/08/22/information-warfare-in-russias-war-in-ukraine/

https://media.defense.gov/2023/Nov/17/2003342901/-1/-1/1/2023-DEPARTMENT-OF-DEFENSE-STRATEGY-FOR-OPERATIONS-IN-THE-INFORMATION-ENVIRONMENT.PDF

https://thediplomat.com/2023/09/chinas-increasingly-aggressive-tactics-for-foreign-disinformation-campaigns/

https://blogs.microsoft.com/on-the-issues/2023/09/07/digital-threats-cyberattacks-east-asia-china-north-korea/

https://www.chathamhouse.org/2023/12/russian-cyber-and-information-warfare-practice

https://taiwaninsight.org/2024/02/05/disinformation-and-civil-defence-how-did-taiwans-civil-society-counter-foreign-information-manipulation/

Cyberwatch Weekly

PUBLISHER
Cyberwatch Finland
Nuijamiestentie 5 C
04400 Helsinki
www.cyberwatchfinland.fi

THE EDITORIAL TEAM
Editor-in-Chief
Aapo Cederberg
aapo@cyberwatchfinland.fi

Subeditor
Elina Turunen
elina@cyberwatchfinland.fi

LAYOUT
Elina Turunen
elina@cyberwatchfinland.fi

ILLUSTRATIONS
Pixabay
Unsplash

A PASSION FOR A SAFE CYBER WORLD

Contact

Cyberwatch Oy
Nuijamiestentie 5C
00400 Helsinki Finland

aapo@cyberwatchfinland.fi
ake@cyberwatchfinland.fi
myynti@cyberwatchfinland.fi